
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# VYLEPŠENÍ ARCHITEKTURY SYSTÉMU SPRÁVY IDENTIT VE FIRMĚ

CORPORATE IDENTITY AND ACCESS MANAGEMENT SYSTEM ARCHITECTURE IMPROVEMENT PROPOSAL

**DIPLOMOVÁ PRÁCE**
MASTER'S THESIS


**AUTOR PRÁCE** — **Bc. Dominik Nop**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR



**BRNO 2019**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání diplomové práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Student: | **Bc. Dominik Nop** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Informační management |
| Vedoucí práce: | **Ing. Viktor Ondrák, Ph.D.** |
| Akademický rok: | 2018/19 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

## Vylepšení architektury systému správy identit ve firmě

**Charakteristika problematiky úkolu:**

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Navrhnout management bezpečnosti v oblasti správy identit.

**Základní literární prameny:**

BERTINO, Elisa a Kenji TAKAHASHI. Identity management: concepts, technologies, and systems. Boston: Artech House, 2011. ISBN 16-080-7039-5.

BISHOP, Matt. Computer security: art and science. Boston: Addison-Wesley, 2003. ISBN 02-01--4099-7.

MADSEN, Paul, Yuzo KOGA a Kenji TAKAHASHI. Federated identity management for protecting users from ID theft. Proceedings of the 2005 workshop on Digital identity management - DIM '05: Proceedings of the 2005 workshop on Digital identity management. New York: ACM Press, 2005. ISBN 1595932321.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

OSMANOGLU, T. Ertem. Identity and access management: business performance through connected intelligence. Amsterdam: Syngress, an imprint of Elsevier, 2013. ISBN 978-012-4081-406.

STAMP, Mark. Information security principles and practice [online]. Hoboken, N.J: Wiley-Interscience, 2005, s. 153-176 [cit. cit. 2016-10-5]. ISBN 9780471744191.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

**Abstrakt**

Tato diplomová práce je zaměřena na posouzení stávající podoby systému správy identit ve firmě a navržení nové podoby za účelem zvýšení úrovně stability a informační bezpečnosti ve společnosti, primárně ve vztahu k systémům zpracovávajícím finanční data. V teoretické části jsou vymezeny základní oborové pojmy a popsány složky a princip fungování systému správy identit. V praktické části je provedena analýza současného stavu. Na základě analýzy jsou navrženy organizační i technické změny, včetně návrhu implementace a provedeno ekonomické zhodnocení celého návrhu.

**Abstract**

The master thesis focuses on assessment of current implementation of identity management system and proposal of a new implementation to increase level of stability and information security in the company, primarily regarding the systems that process financial data. In first part, basic theoretical knowledge related to identity management systems is defined. In second part, an analysis of current system state is performed. Based on this analysis, new organizational and technical solutions are proposed to the company. Finally, an implementation project proposal as well as with risk analysis and economic evaluation is completed in the end of this thesis.

**Klíčová slova**

správa identit, autentizace, heslo, přístup, role, Kerberos, SSO, provisioning

**Keywords**

Identity management, authentication, password, access, role, Kerberos, provisioning

**Bibliografická citace**

NOP, Dominik. Vylepšení architektury systému správy identit ve firmě [online]. Brno, 2019 [cit. 2019-05-10]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/116147. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

**Čestné prohlášení**

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2019

.....

podpis studenta

**Poděkování**

Děkuji vedoucímu mé práce, Ing. Viktoru Ondrákovi, Ph.D. za veškeré rady, připomínky a čas věnovaný této práci. Dále děkuji panu Igoru Gricinkovi, MBA za konzultace a za poskytnuté doplňující informace.

# OBSAH

# ÚVOD

S rozmachem internetových služeb roste i počet tzv. startupů – začínajících podnikatelských subjektů s rychlým stupněm vývoje. Tyto subjekty využívají svoji flexibilitu a neformálnost v rámci interních i externích procesů k zajištění rychlé expanze na trhu. Po určitém čase ale každý úspěšný podnik musí přejít na více organizovanou strukturu, aby stabilizoval svůj vývoj dříve, než ztratí iniciativu z počáteční fáze svého životního cyklu. Nedílnou součástí stabilizace je i standardizace a formalizace interních procesů. Správa identit patří mezi důležité interní procesy, které je potřeba formalizovat, pro zajištění interní stability i bezpečnosti relevantních procesů. Tato práce se zabývá vylepšením systému správy identit formalizací relevantních procesů.

# CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této práce je navrhnout vylepšení systému správy identit ve společnosti ABC, s.r.o. z hlediska formalizace, standardizace i kvality technických řešení. Důsledkem bude zvýšení bezpečnosti a snížení uživatelské náročnosti každodenních procesů, zajištění informovanosti všech zaujatých stran v rámci společnosti a zajištění transparentnosti pro externí subjekty, např. auditory. Dalším cílem práce je zajistit bezproblémovou implementaci prostřednictvím metod projektového řízení, včetně řízení potenciálních rizik, souvisejících s implementací.

# 1 TEORETICKÁ VÝCHODISKA PRÁCE

V této části práce uvedu základní pojmy související s tématem a zaměřením práce.

## 1.1 Identita

Definice identity je nezbytná pro možnost definovat Identity management. Identita je definována doporučením ITU Y.2720 [1] jako informace o entitě, skládající se z identifikátoru, atributu a tzv. credential (volně lze přeložit jako ověřovací údaj nebo pověřovací atribut, viz níže). Tyto informace jsou dostačující pro identifikaci entity bez vlivu dalších informací. Entitou podle M. Bishopa [2] může být osoba, budova, stroj nebo jiný umělý, nebo přírodní objekt.

Jedna entita může mít současně více identit, každá z identit reprezentuje jinou část entity. Soukromý a zaměstnanecký účet osoby reprezentují každý jinou část jeho osobnosti. Identity lze vzájemně propojovat a usnadnit tak uživateli práci (více v následujících podkapitolách) [3].

### 1.1.1 Identifikátor

Identifikátor je podle ITU-T Y.2720 [1] posloupnost číslic, písmen, symbolů a dalších druhů dat, užívaná pro identifikaci jednoho nebo více uživatelů, síťových elementů, funkcí, síťových entit, poskytovaných služeb, odběratelů a dalších entit. Příkladem je jméno uživatelského účtu, zaměstnanecké ID, číslo dokladu apod.

### 1.1.2 Credential

Credential (ověřovací údaj) je podle ITU-T Y.2720 [1] identifikovatelný objekt, použitelný pro autentizaci i autorizaci žadatele. Mezi ověřovací údaje patří hesla, otisky prstů, digitální certifikáty apod.

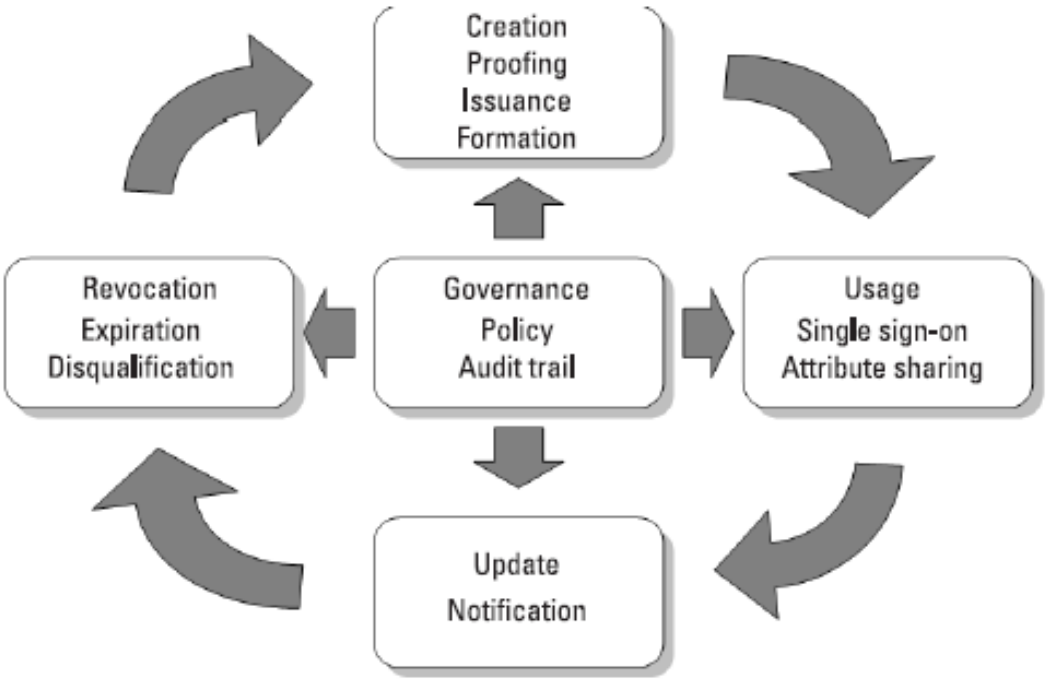
### 1.1.3 Atribut

ITU-T Y.2720 [1] definuje atribut jako popisující informaci, přímo vázanou na danou entitu, specifikující její konkrétní vlastnost, např. stav, kvalitu. U osob jde např. o celé jméno, rodinný stav, titul, pohlaví, bydliště apod.

## 1.2 Identity management

Identity management je soubor procesů, které spravují identity v průběhu celého jejich životního cyklu za účelem zajištění jejich relevantnosti pro ověřovací systémy služeb bezpečným a diskrétním způsobem. Bezpečný způsob je takový, který zajistí důvěrnost, dostupnost i integritu. Diskrétností z pohledu správy identit rozumíme zajištění práva entity svobodně manipulovat s vlastními identitami. Z pohledu síťových transakcí jde o zaručení, že entita může kontrolovat, jak moc je možné spojit jednotlivé požadavky od služeb, bez ohledu na jejich reálnou míru vzájemné provázanosti [4].

Životní cyklus identity se skládá z jejího vytvoření, užívání, aktualizace a revokace. Ve všech fázích musí být identita efektivně spravována [3]. V následujících podkapitolách rozeberu jednotlivé fáze.




**Obr. 1: Životní cyklus identity**

(Zdroj: 3)

### 1.2.1 Vznik identity

Založení identity probíhá ve 3 fázích – prokázání atributů, přidělení credentials a vygenerování identity [3].

Prokázání atributů je prováděno ověřením oprávněnou autoritou – např. ověření věku místními úřady, nejčastěji prostřednictvím občanského průkazu. K tomuto kroku nedochází ve všech případech, např. při zakládání účtu na většině webových stránek nedochází k ověření atributů. Výsledkem jsou falešné profily (velmi běžné např. na sociálních sítích) [3].

K přidělení credentials dochází po prokázání atributů. Credentials jsou přiděleny oprávněnou autoritou (např. digitální certifikáty), nebo si je může entita vytvořit sama

(heslo, PIN). Příjemce credentials musí být informován, kdo a kdy může credentials přidělit a kdy dojde k jejich vypršení [3].

Ve finální fázi dojde k vytvoření identifikátoru žadatele poskytovatelem identity. Prokázané atributy a přidělené credentials, společně s identifikátorem dohromady tvoří novou identitu. Identifikátor musí být pro uživatele snadno zapamatovatelný. Pokud je použit pseudonym, je zvýšena úroveň soukromí entity. Vyšší úrovně diskrétnosti lze dosáhnout použitím různých pseudonymů pro různé druhy transakcí [3].

### 1.2.2 Užívání identity

Identita umožňuje jejímu vlastníkovi využívat služby poskytované zakladatelem. Pro zajištění bezpečného i diskrétního využití identity, využívají služby poskytované na základě identity tyto funkce: důvěryhodnou komunikaci, SSO a sdílení atributů [3].

Důvěryhodnou komunikaci lze zjistit, rozpoznat a autentizovat odesílatele i příjemce zpráv. Volba příslušného mechanismu závisí na jeho škálovatelnosti a bezpečnosti [3].

Single sign-on (SSO) je transakce umožňující využití výsledků autentizace pro více než jednu službu. Pokud má uživatel veškerá potřebná oprávnění, může využívat veškeré služby, které danou verzi SSO podporují a jsou správným způsobem nakonfigurovány. Jednotná autentizace snižuje nároky na uživatele ohledně počtu hesel a identit, které musí spravovat, ale v případě prolomení zabezpečení zvyšuje dopad útoku [6].

Sdílení atributů je transakce, která umožňuje poskytovateli identit sdílet atributy jím spravovaných identit s poskytovateli služeb. Jednotná verze atributů zamezuje vzniku redundancí a nekonzistencí mezi údaji uloženými u jednotlivých služeb v síti. Pro sdílení atributů je nezbytný souhlas jejich nositele, formou běžné interakce, nebo předem podepsanou dohodou. Vlastník identity musí být informován o důvodech sdílení, cílových subjektech, se kterými budou atributy sdíleny a době trvání sdílení [3].

### 1.2.3 Aktualizace identity

Údaje o identitě jsou aktualizovány průběžně, po celou dobu její existence. K aktualizaci musí docházet pravidelně pro zachování integrity identity. V případě sdílení atributů musí být sdíleny i veškeré dodatečné změny v údajích. Veškeré změny musí být logovány pro případné pozdější dohledání v rámci auditních procedur. Klíčové identifikátory musí být nadefinovány tak, aby mohly zůstat nezměněné po celou dobu existence identity. To umožňuje dohledání identity v jakékoli fázi nehledě na množství změn u ostatních atributů [7].

### 1.2.4 Revokace identity

Každá entita musí mít identitu vytvořenou pouze na dobu, po kterou ji potřebuje. V případě ztráty podstaty existence identity (např. ukončení pracovního poměru se zaměstnancem, disponujícím identitou v Active Directory) musí být identita neprodleně zrušena, nebo zablokována. To samé platí pro případ kompromitace nebo krádeže credentials. O revokaci musí být informován vlastník identity i služby, se kterými jsou údaje o identitě sdíleny. Revokace musí být následně zaznamenána pro případné dohledání v rámci auditních procedur. Systém ve firemním prostředí by měl mít implementovanou revizi uživatelských účtů, při které revidující osoba ověří, že se mezi účty nenachází tzv. dormanti – aktivní účty patřící zaměstnancům, se kterými byl ukončen pracovní poměr [3].

### 1.2.5 Řízení identity

Řízení je spojeno se všemi fázemi životního cyklu identity. Všechny transakce musí být řízeny příslušnými směrnicemi a musí být zaznamenávány. Tyto směrnice bývají

implementovány např. v rámci metodik SOX nebo ISO 27000. Směrnice zahrnují nároky na autentizaci (např. parametry pro sílu hesla), procesy pro přidělování přístupů a oprávnění, jejich změnu i revokaci. Poskytovatelé služeb mohou mít vlastní směrnice, které musí být brány v potaz. Součástí směrnic musí být i informování o způsobech vynucení, např. nastavením politiky hesel v Active Directory [3]. V rámci implementace pak může být využito řízení přístupů na základě rolí (RBAC, viz níže) [8].

## 1.3 Stakeholdeři v procesu správy identit

V procesu správy identit je několik zainteresovaných stran, které rozeberu v této podkapitole.

### 1.3.1 Subjekt

Subjektem rozumíme entitu, která poskytuje své atributy v digitální podobě pro potřeby získání přístupu ke službám. Jejich důležitým požadavkem je ochrana soukromí a ochrana proti zneužití [3].

### 1.3.2 Poskytovatel identity

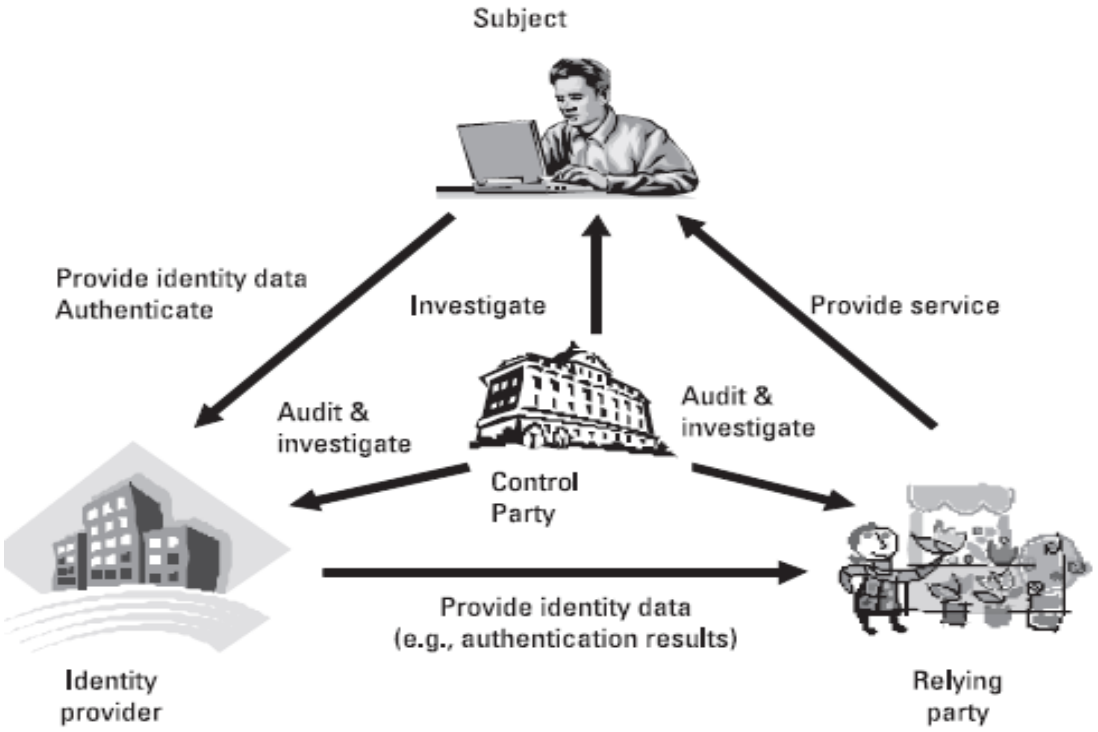
Poskytovatel identity generuje a přiděluje atributy identity subjektům. Dále u subjektu zajišťuje případné vazby mezi jednotlivými atributy včetně atributů od jiných poskytovatelů (např. pro založení bankovního konta je potřeba poskytnou bance kopii občanského průkazu). V případě standardů typu SAML, OpenID apod. poskytuje i tzv. tvrzení (assertion) poskytovatelům služeb pro zajištění jednotného přihlášení (více v následujících podkapitolách). Pro poskytovatele je důležitým požadavkem zajištění důvěryhodnosti atributů identity od jiných poskytovatelů i jejich tvrzení [3].

### 1.3.3 Poskytovatel služeb

Poskytovatel služeb zajišťuje subjektu přístup ke svým zdrojům nebo službám na základě credentials subjektu. Důležitá pro tuto zainteresovanou stranu je schopnost určit důvěryhodnost poskytnutých credentials, atributů nebo tvrzení od poskytovatelů identit. Různé služby vyžadují různou úroveň důvěryhodnosti, na základě iniciativy poskytovatele i různých legislativních a regulačních opatření. Poskytovatel musí z tohoto důvodu mít možnost ověření atributů u jejich poskytovatele [3].

### 1.3.4 Kontrolní skupiny

U některých zainteresovaných skupin může vzniknout potřeba přístupu k informacím o identitě, typicky pro potřeby investigativní, nebo auditní účely. Nejčastěji se jedná o policejní útvary, regulátory a auditory. Pro tyto skupiny je důležité zajištění transparentnosti [3].




**Obr. 2: Vazby mezi jednotlivými stakeholdery**

(Zdroj: 3)

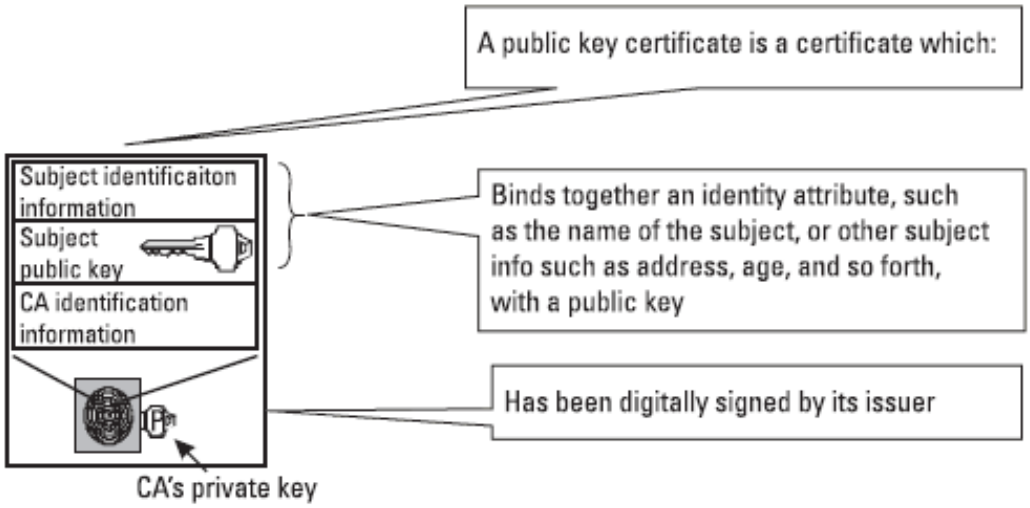
## 1.4 Řešení a technologie v oblasti credentials

U credentials je důležité zajištění jejich integrity a platnosti. Zachování integrity znamená, že s údajem nebylo nijak manipulováno. Pro tyto účely slouží např. digitální certifikáty. Platností rozumíme pravdivost obsahu credentials [3].

### 1.4.1 Digitální certifikáty a asymetrická kryptografie

Certifikáty spojují atributy identity s veřejným klíčem asymetrické kryptografie. Veřejný klíč se používá k šifrování zpráv. Dešifrování je možné pouze s pomocí soukromého klíče, který je matematicky propojen s klíčem veřejným. Každý může zprávu s pomocí veřejného klíče zašifrovat, ale pouze vlastník soukromého klíče může zprávu dešifrovat.

Opačný postup lze použít k identifikaci nebo autentizaci entity a používá se k udělení certifikátu tzv. certifikační autoritou (CA). Certifikační autorita zašifrovaný dokument podepíše svým soukromým klíčem. Použitím veřejného klíče této autority příjemce ví, že CA dokument podepsala [9].




**Obr. 3: Digitální certifikát**

(Zdroj: 3)

Certifikát je založen na standardu X.509 a obsahuje následující komponenty [9]:

- Verze (1, 2, nebo 3)
- Sériové číslo
- Identifikátor algoritmu digitálního podpisu
- Jméno CA podle X.500
- Doba platnosti
- Jméno subjektu podle X.500 (tzv. Distinguished name – DN), obsahující následující:
    - Common name (CN)
    - Organizace nebo společnost
    - Organizační jednotka (OU – organization unit)
    - Město/lokalita

- Stát/provincie
- Země
- Informace o veřejném klíči (algoritmus, parametry, klíč)
- Unikátní identifikátor poskytovatele (od verze 2)
- Unikátní identifikátor entity (od verze 2)
- Prostor pro rozšíření (od verze 3)
- Podpis (hash všech polí v certifikátu)

Pro vydání certifikátu se žadatel musí zaregistrovat u CA. Během registrace dojde k autentizaci. Poté je vygenerován pár klíčů (soukromý a veřejný), které budou využity pro certifikaci. Certifikát společně s vygenerovaným veřejným klíčem jsou zaslány žadateli [9].

### 1.4.2 Atributové a autorizační certifikáty

Princip fungování je podobný jako u certifikátů založených na veřejném klíči. Atributové a autorizační certifikáty nepoužívají veřejný klíč, ale široké spektrum atributů dané entity. Tento certifikát ujišťuje poskytovatele služeb o autorizaci subjektu k přistoupení k jeho zdrojům a službám. Tento druh certifikátu je používán např. v tzv. tvrzeních SAML – Security Assertion Markup Language [10].

### 1.4.3 Sdílení credentials

Ke sdílení credentials dochází v situaci, kdy subjekt A pověří subjekt B v používání jeho credentials k přístupu ke zdrojům a službám. Potřeba sdílení vzniká v situaci, kdy jsou ze subjektu A delegovány odpovědnosti za určité činnosti na subjekt B, ale subjekt B nemá nastavenou odpovídající úroveň důvěry s třetí stranou, potřebnou pro vykonání dané činnosti. Subjekt B proto ohlásí, že jedná jménem subjektu A, který danou úroveň důvěry s třetí stranou má [11].

Problémem je zajištění ověření, že subjekt B skutečně jedná jménem subjektu A. Jednou z možností je dotaz třetí strany na subjekt A. Takový proces je náročný, kvůli potřebě autentizace pro každou individuální žádost. Druhou možností je poskytnutí soukromého klíče vlastněného subjektem A subjektu B. Toto řešení není bezpečné, proto nejčastěji subjekt A předává místo klíče certifikát [11].

## 1.5 Single sign-on (SSO)

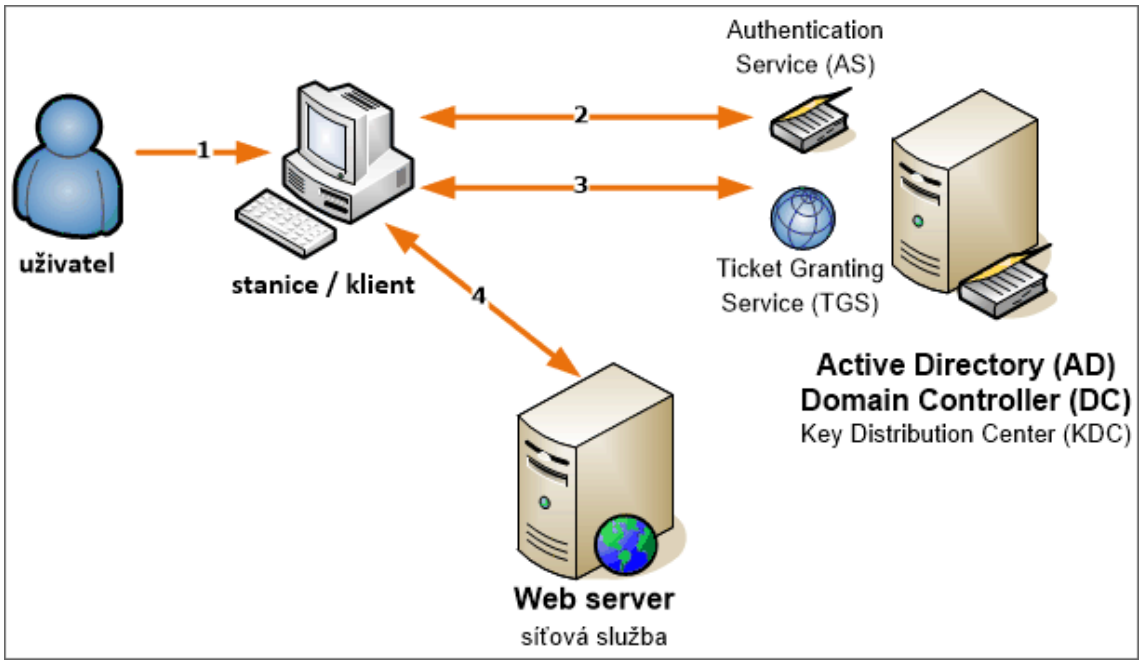
Single sign-on je systém pro zajištění jednotného přihlášení. Subjekt pro potřebu využití většího množství služeb a zdrojů autentizuje pouze jednou za relaci. Nejde o sjednocení uživatelských přihlašovacích údajů, ale o jejich mapování na jediný účet. SSO může být zavedeno v rámci společnosti (Enterprise SSO – ESSO), v rámci více domén (multidoménové SSO – MSSO), nebo v rámci Internetu (Web-based SSO). Většina dnešních řešení je typu ESSO [12]. V této podkapitole rozeberu druhy SSO podle jejich architektury.

### 1.5.1 Architektura založená na zprostředkovateli (Broker-based)

Jádrem této architektury je centrální prvek, který slouží jako zprostředkovatel (broker) v autentizačním procesu. Tato třetí strana provádí prvotní ověření identity subjektu a vydává tickety ostatním službám. Subjekt se po prvotní autentizaci vůči třetí straně dále autentizuje s pomocí těchto ticketů. Uživatel přitom nevykonává žádnou činnost, autentizace probíhá automaticky při žádosti subjektu o přístup [6].

Příkladem je integrovaná služba Active Directory, protokol Kerberos. Jeho centrální prvek obsahuje 2 služby – Ticket Granting Server (TGS) a Authentication Server (AS). Subjekt odešle žádost AS obsahující jeho identifikátor. V reakci je mu přidělen Ticket-Granting Ticket (TGT), zašifrovaný způsobem, který zvládne dešifrovat pouze TGS + session key, zašifrovaný tajným klíčem subjektu (nejčastěji uživatelské heslo). Subjekt

zašle žádost na TGS, obsahující TGT a dešifrovaný Session key. Odesláním dešifrovaného session key se vůči serveru autentizuje bez zaslání hesla. TGS na základě TGT a session key vydá subjektu service ticket, zašifrovaný tajným klíčem poskytovatele služby, ke které má subjekt v úmyslu přistoupit. Subjekt pošle service ticket poskytovateli společně s časovým razítkem. Poskytovatel obě zprávy dešifruje a pošle subjektu navýšené časové razítko pro zajištění vzájemného ověření a důvěry [13].




**Obr. 4: Kerberos autentizace**

(Zdroj: 13)

Alternativním řešením v oblasti zprostředkovatelského SSO je SESAME. Ten využívá asymetrickou kryptografii pro distribuci klíčů – Kerberos užívá symetrickou. Dále SESAME nepředává po autentizaci subjektu tickety, používá certifikáty, kterými subjekt autentizuje i autorizuje k použití služeb [14].

Výhodou i nevýhodou této architektury je centralizace citlivých údajů do jediného serveru. Architektura usnadňuje správu a zajišťuje oboustrannou autentizaci, centralizace ale současně zvyšuje dopad případného útoku na systém. Některé autentizační procesy jsou ale bezpečnější oproti běžným, např. credentials jsou posílány na server pouze při prvotní komunikaci pro potřeby uložení do databáze. Další nevýhodou této formy centralizace je potřeba sjednocení autentizačních metod [14].

### 1.5.2 Architektura založená na agentovi (Agent-based)

Agentem je podle [14] rozuměn program, který autentizuje identity subjektu vůči různým aplikacím. Agent funguje jako překladač autentizačních metod mezi subjektem a aplikacemi (např. převod heslového mechanismu na X.509 certifikáty).

Agent zajišťuje decentralizaci přístupových procesů a zachovává tak úroveň bezpečnosti. Zároveň není vázán na jedinou autentizační metodu, na rozdíl od zprostředkovatele. Nevýhodou architektury je náročnost na správu agenta, u kterého je nutné upravovat design pro různé aplikace. Dalším problémem je potřeba implementace nového agenta ke každé nové aplikaci [14].

### 1.5.3 Hybridní architektura (Agent and broker-based)

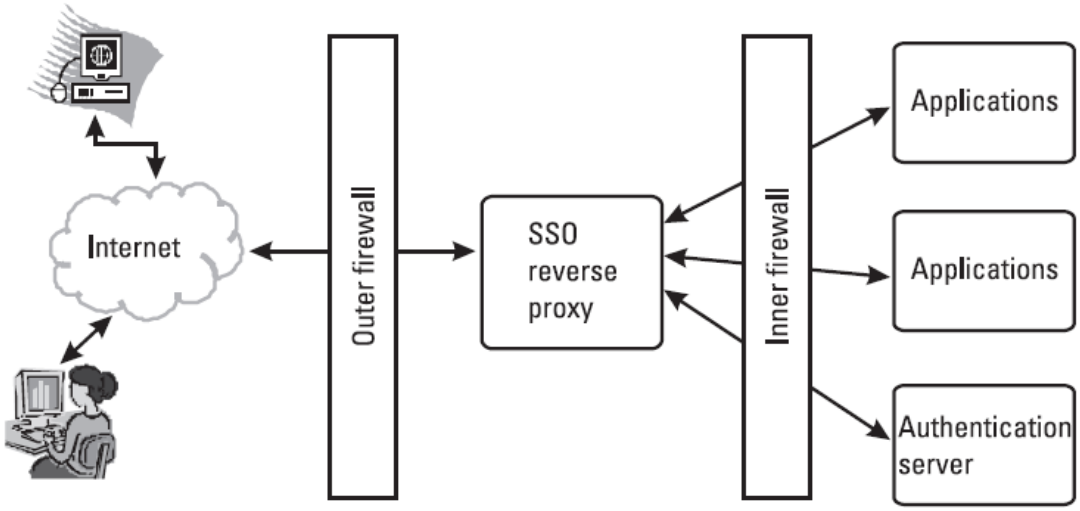
Hybridní architektura je kombinací předchozích dvou. Implementace centrálního autentizačního zprostředkovatele i agenta dodá systému flexibilitu při zachování centrální správy. Kromě výhod zůstává i problém vysokého dopadu při napadení centrálního prvku a potřeba implementace nového agenta pro novou aplikaci [15].

### 1.5.4 Architektura založená na tokenu (Token-based)

Subjekt, který v této architektuře chce přistoupit ke zdrojům poskytovatele služeb, se poprvé autentizuje zadáním správných credentials. V reakci kromě autorizace obdrží subjekt tzv. token. Ten může být využit při další žádosti subjektu vůči dané službě. Token obsahuje informace potřebné k identifikaci subjektu při další komunikaci a nahrazuje opakované zasílání credentials. Token má omezenou dobu platnosti. Tento model SSO je snadný na vytvoření, ale nevhodný z bezpečnostního hlediska [15].

### 1.5.5 Reverzní Proxy architektura (Reverse Proxy-based)

Řešení je využívané pro externí přístup do sítě. Autentizační proces probíhá na vstupním bodě do sítě, typicky v demilitarizované zóně (DMZ). „Brána“ filtruje externí uživatelské credentials a povoluje přístup ke službám pouze subjektu s platnými credentials. Bez platných údajů je subjekt přesměrován na systém nebo aplikaci pověřenou přidělováním platných credentials, kde je zahájen proces autentizace. [16].




**Obr. 5: Reverzní proxy architektura**

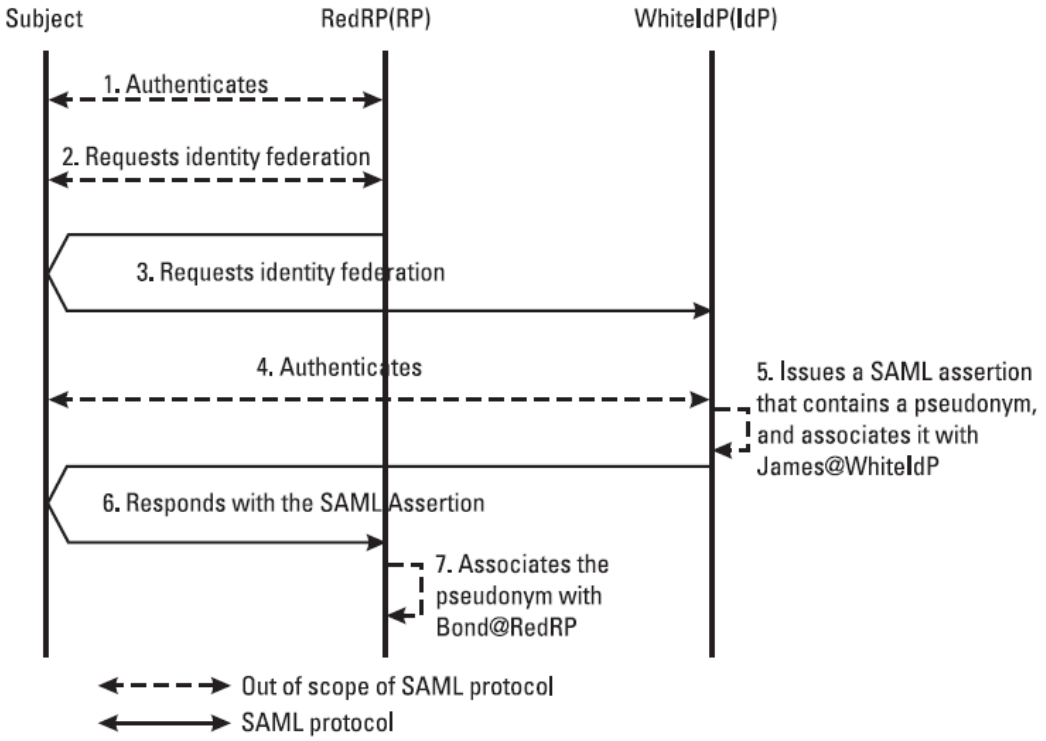
(Zdroj: 16)

## 1.6 Standardy v oblasti IdM

V této podkapitole uvedu v současné době nejrozšířenější standardy v oblasti správy identit.

### 1.6.1 SAML

SAML (Security Assertion Markup Language) je soubor technických specifikací pro správu identit na základě jejich sdružování (identity federation). Jeden subjekt, vlastnící více identit, spravovaných různými poskytovateli, může užitím SAML vytvářet, měnit a rušit vazby mezi nimi při současném užívání webového mechanismu jednotného přihlášení – Web SSO. Poskytovatel služby obdrží od poskytovatele identity prostřednictvím http přesměrování tzv. tvrzení (assertion) o subjektu, který žádá přístup ke službě. Tvrzení nahrazuje individuální autentizační mechanismy poskytovatele služeb a může být použito v rámci všech subjektem nastavených vazeb. SAML pracuje na principu minimálního sdílení informací o vazbách mezi identitami prostřednictvím pseudonymizace [17].




**Obr. 6: Autentizace v SAML 2.0**

(Zdroj: 3)

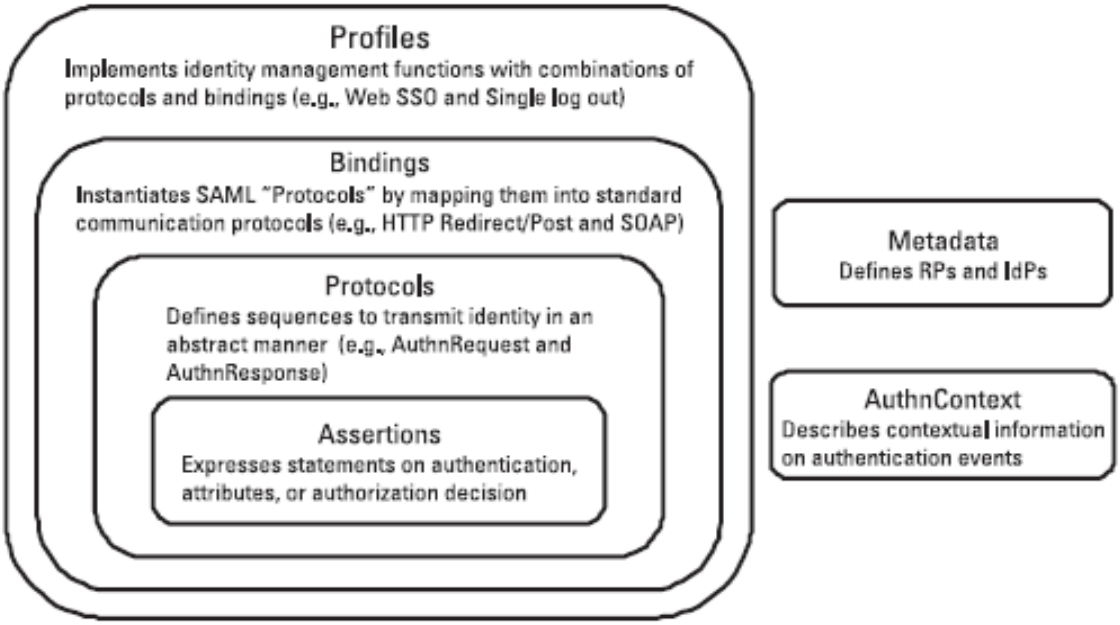
Aktuální verze SAML je 2.0. Specifikace této verze se skládá ze 4 vrstev – tvrzení, protokol, vazba a profil [17].

Vrstva tvrzení (assertion) je jádrem SAML komunikace. Tvrzení je vydáno a podepsáno poskytovatelem identity a předává poskytovateli služby 3 druhy informací – autentizaci

(tj. způsob, kterým byl subjekt autentizován poskytovatelem identity), rozhodnutí o autorizaci a atribut. Tvrzení jsou posílána všem poskytovatelům služeb v rámci stanovených vazeb a umožňují nositeli identity přistoupit ke službám poskytovatelů bez další autentizace [17].

Další vrstvy specifikují způsob zpracování tvrzení. Na protokolové vrstvě jsou definovány používané druhy SAML zpráv. Na vrstvě vazby je určen způsob zapouzdření SAML zprávy pro zajištění kompatibility s některým ze standardních komunikačních protokolů – např. http. Na vrstvě profilu se definuje použití dané kombinace tvrzení, protokolu a vazby pro konkrétní funkci [17].

V rámci protokolu SAML jsou důležitá i tzv. metadata. Slouží k definování požadované úrovně důvěry mezi poskytovatelem identity a poskytovatelem služby. Mezi metadata patří digitální certifikáty nebo SAML vazby [17].



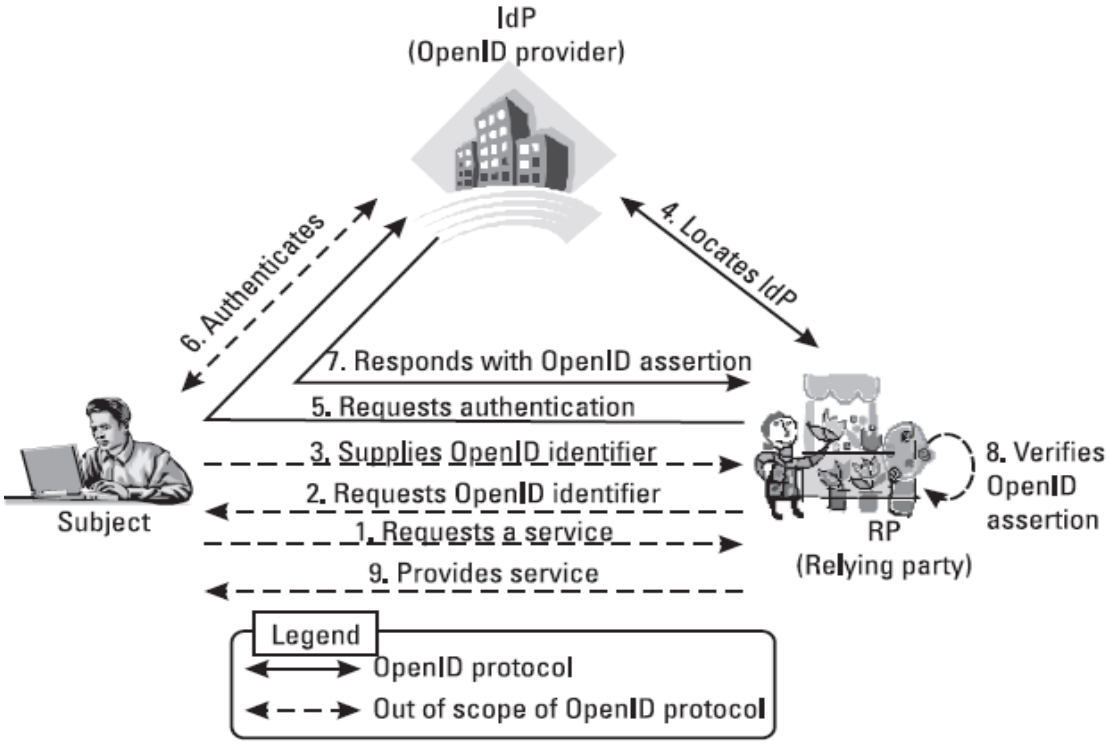

**Obr. 7: Struktura SAML 2.0**

(Zdroj: 3)

.

### 1.6.2 OpenID

OpenID je řešení založené na reprezentaci identity (nebo subjektu) v podobě URI. Autentizační proces se podobá řešení SAML 2.0. OpenID ale na rozdíl od SAML umožňuje subjektu zvolit si poskytovatele identity při každé autentizaci. Dalším rozdílem je jednoduchost – OpenID má jednodušší strukturu dat, která jsou odesílána v rámci tvrzení, např. výsledek autentizace je „succeeded“ nebo „failed.“ Řešení bylo navrženo pro webové aplikace a systémy s nižšími požadavky na bezpečnost, např. blogy [18].




**Obr. 8: Princip fungování OpenID**

(Zdroj: 3)

Stejně jako u SAML 2.0, tvrzení mezi poskytovatelem identity a poskytovatelem služeb jsou předány přes http přesměrování. Poskytovatele identit volí subjekt. Poskytovatel služeb zjistí jeho lokaci jedním ze tří mechanismů – Extensible Resource Indicator (XRI), protokol Yadis, nebo vyhledávání na základě HTML. Pro zajištění bezpečné komunikace

mohou být mezi poskytovatelem identit a služeb vyměněny klíče metodou Diffie-Hellman pro zajištění šifrované komunikace.

# 2 Analýza současného stavu

V této kapitole stručně představím společnost a popíšu současný stav systému správy identit a souvisejících entit a procesů.

## 2.1 O společnosti

ABC a.s. je společnost, zaměřená na internetový obchod s oblečením. Sídlo společnosti se nachází v Praze. Výdejny má společnost v Praze, Brně, Plzni a v Hradci Králové. Na Slovensku pak je pouze pobočka v Trenčíně. V dalších městech – především na Moravě, ve Slezsku a na Slovensku – firma spolupracuje s výdejnami. V současnosti zaměstnává společnost okolo 80 zaměstnanců.

## 2.2 Analýza vnitřních faktorů – model 7S

V této podkapitole provedu vnitřní analýzu podniku s pomocí analýzy 7S. Ta zohledňuje následující oblasti [19]:

- Strategie
- (Organizační) Struktura
- (Informační) Systémy
- Styl řízení
- Spolupracovníci
- Sdílené hodnoty
- Schopnosti

### 2.2.1 Strategie

Strategie firmy je založená na snaze odlišit se způsobem prodeje zboží, současně je snahou firmy prodávat zboží za nízké ceny v porovnání s konkurencí.

U procesu prodeje zboží je snaha zajistit zákazníkovi co nejvyšší komfort. Zákazník může nakupovat z pohodlí domova prostřednictvím e-shopu společnosti. Nabídky může dostávat přes newslettery zasílané emailem, nebo přes sociální sítě. Zákazník může zaplatit až po vyzkoušení produktu v místě odběru, pokud jde o pobočku firmy. Zákazník, který odebírá zboží v odběrovém místě partnerských firem, může zboží vrátit s plnou náhradou ceny. Podmínkou je vrácení nepoškozeného zboží.

Kromě toho se společnost snaží poskytovat levnější zboží oproti konkurenci prostřednictvím slev a voucherů. Podle interních průzkumů je touto cestou prodáno cca 80% zboží. Nejčastější formou doručování slev je zasílání slevových kódu na určité druhy zboží v závislosti na jeho množství ve skladech, aktuálních cenách u konkurence a dalších faktorech. Zákazník, který zažádal o odběr novinek, dostává prostřednictvím emailu cca dvakrát do týdne slevový kód. Některé slevy jsou zveřejňovány na sociálních sítích.

Hlavním příjmem společnosti je prodej licencovaných značek. Společnost navrhuje i vlastní značky výrobků a postupně zvyšuje jejich podíl na celkových příjmech firmy. Momentálně jsou ale výdaje na vývoj vlastní značky vyšší než výdaje na licencované značky. Toto firma plánuje v budoucnu změnit zvyšováním objemu vlastní produkce a snižováním podílu fixních nákladů na nákladech celkových.

### 2.2.2 Struktura

Na vrcholu firmy stojí výkonný ředitel společnosti a finanční ředitel. O úroveň níže jsou vedoucí jednotlivých oddělení. Pod ně spadají jednotliví zaměstnanci. Některá početnější oddělení mají u jednotlivých skupin zaměstnanců (např. designéři a grafici) team leadery – zkušenější zaměstnance spadající pod vedoucího oddělení, na které jsou delegovány některé odpovědnosti a pravomoci v oblasti operativního managementu. Organizační strukturu společnosti ABC přikládám do příloh.

Team leadeři nejsou formálně nadřízenými ostatních zaměstnanců v oddělení, patří do jednotlivých oddělení. Vedoucí oddělení jsou formálními nadřízenými.

### 2.2.3 Systémy

Systémy ve společnosti analyzuji v samostatných podkapitolách.

### 2.2.4 Styl řízení

Každý zaměstnanec má možnost předložit návrh na zlepšení v jakékoli oblasti. Rozhodnutí na celofiremní úrovni ale provádí ředitel společnosti po poradě se zainteresovanými stranami, především s CFO. Pravomoci a odpovědnosti na úrovni oddělení jsou delegovány na vedoucí oddělení, např. jednání s poskytovateli služeb.

Společnost dopřává svým zaměstnancům velkou míru volnosti. Zaměstnanci nejsou vázáni výraznější firemní byrokracií. To podporuje kreativitu designérů a celkově odstraňuje stereotypizaci práce. Důsledkem byl v minulosti rychlý start na výrazně konkurenčním prostředí.

Nízká úroveň organizování a řízení je nyní pro firmu, která se v současnosti na trhu snaží pevně usadit, spíše problémem, který může v budoucnu způsobit destabilizaci podniku.

### 2.2.5 Spolupracovníci

Firma má v současnosti přibližně 80 zaměstnanců. Cca třetinu tvoří zaměstnanci marketingového a obsahového oddělení, které generuje nejvyšší příjmy. IT oddělení, na

kterém bude tato práce založena, tvoří cca 10 zaměstnanců. Většina zaměstnanců společnosti je mladších 35 let, velká část z nich vstoupila do společnosti jako absolventi.

V budoucnu se plánuje expanze výrobního oddělení v rámci snahy o zvýšení celkové firemní podpory vlastní značky.

### 2.2.6 Sdílené hodnoty

Ve společnosti panuje uvolněná kultura – žádný dress code, pracovní procesy se zpravidla neformalizují. Pokud ale v některém případě k formalizaci dojde, je striktně dodržována. Zaměstnanci si cení uvolněného prostředí, ale vnímají, že nízká organizovanost vede ke zmatkům v procesech a k neefektivitám a jsou otevření změnám v této oblasti.

Hlavním cílem společnosti je expandovat na českém i slovenském trhu a rozšířit svoji síť poboček. Dalším cílem je rozšířit portfolio prodávaných produktů a značek, při současné preferenci vlastních značek před licencovanými. Zaměstnanci jsou o směřování společnosti informování při výběrovém řízení a s těmito cíli se převážně ztotožňují.

### 2.2.7 Schopnosti

Zaměstnanci jsou převážně nižšího věku, s minimem předchozích zkušeností. Jejich největší předností je kreativita, znalosti nejnovějších módních trendů a schopnost přemýšlet „outside the box.“ Všichni zaměstnanci absolvovali kurzy BOZP. Někteří zaměstnanci IT oddělení mají zkušenosti s implementací SOX z dřívějších zaměstnání.

## 2.3 Analýza vnějších faktorů – SLEPT analýza

V této podkapitole provedu analýzu vnějšího okolí SLEPT, ta zohledňuje následující faktory [19]:

- Sociální
- Legislativní
- Ekonomické
- Politické
- Technologické

### 2.3.1 Sociální faktory

Firma má sídlo a fakturační adresu v Praze, odběrová místa na více místech ČR a v Trenčíně na Slovensku. Praha je vhodnou lokalitou pro hledání pracovní síly z řad absolventů. Absolventi tvoří většinu nově příchozích zaměstnanců. Problémem je nízká nezaměstnanost v ČR – nalezení kvalitních pracovníků na trhu práce je náročné.

Cílovými segmenty podnikatelského záměru jsou lidé využívající nákupy po internetu, především studenti. Starší a počítačově negramotní zákazníci nejsou důležitým cílem. Pro firmu je nejvýhodnější situovat výdejny do univerzitních měst. Společnost zvolila odpovídající lokace – Praha, Brno, Plzeň, Hradec Králové a v Trenčín. Vhodným cílem další expanze je Olomouc, Ostrava, Pardubice a České Budějovice. Na Slovensku je vhodným městem pro výdejnu Bratislava a Žilina

### 2.3.2 Legislativní faktory

Firma dodržuje legislativu České republiky a v Trenčíně legislativu Slovenské republiky. Společnost se nedávno přizpůsobovala Evropské regulaci o ochraně osobních údajů – GDPR. Důsledkem byly rozsáhlé úpravy údajů o zákaznících.

Problémem je nedostatek ústavních soudců na Slovensku, který nastal odchodem 13 soudců v polovině února 2019. Důsledkem je paralyzace ústavního soudu na Slovensku a případné problémy při snaze vymáhat dodržování zákonů ze strany stakeholderů na Slovensku.

### 2.3.3 Ekonomické faktory

Česká republika po zotavení se z ekonomické krize z roku 2008 hospodaří s relativně nízkým nebo žádným schodkem. Míra inflace je regulovaná centrální bankou a měna byla dlouhou dobu uměle držena ve stabilním kurzu vůči euru. Daňové sazby se výrazněji nemění, v minulosti existovaly úvahy o jejich snížení, momentálně žádná snaha o jejich změnu není. V předchozích letech rostlo HDP České republiky rychleji než většině ostatních zemí EU, v současnosti hospodářský růst zpomaluje.

### 2.3.4 Politické faktory

ČR je členem EU a podporuje snahy firem čerpat Evropské dotace. Společnost je politicky stabilní, v zemi nejsou výraznější snahy o změnu režimu. Země v současnosti vysílá své vojáky na mise do Afghánistánu, Iráku, Mali atd., ve válečném stavu ani v konfliktu se sousedními zeměmi ale země není. Společnosti nejsou politikou výrazněji ovlivňovány, pokud se nezabývají státními zakázkami. Pro společnost ABC takové zakázky nejsou relevantní, politické faktory nemají další výraznější vliv na působení společnosti.

### 2.3.5 Technologické faktory

Česká republika (resp. výzkumné subjekty působící na jejím území) získává rozsáhlé dotace na výzkum a vývoj od Evropské Unie. ČR ale není významným světovým trhem a nové technologie vynalezené v zahraničí se na tento trh často dostávají s časovým odstupem (např. informační technologie). Přesto se ČR řadí mezi vyspělé země a společnosti nejsou výrazněji omezovány ve volbě technologie.

## 2.4 SWOT analýza

Na základě předchozí analýzy vnitřního i vnějšího prostředí společnosti vypracuji SWOT analýzu. Posoudím nejvýznamnější silné a slabé stránky společnosti a její příležitosti i hrozby do budoucna. Na základě SWOT analýzy rozhodnu o tom, zda je vhodné projekt změny ve společnosti realizovat

**Tabulka 1: SWOT Analýza**

(Zdroj: Vlastní zpracování)

| Silné stránky | Slabé stránky |
|---|---|
| Cílová skupina produktů shodná s cílovou skupinou pro nábor do firmy<br>Kreativní, inovativní a přizpůsobiví zaměstnanci<br>Centrála a výdejny v regionálních centrech<br>Dobré vztahy s poskytovateli licencí<br>Vlastní značka | Nezkušení zaměstnanci<br>Vlastní produkty jsou málo známé<br>Stagnace v IT technologiích<br>Malá úroveň organizování uvnitř firmy |
| **Příležitosti** | **Hrozby** |
| Získání talentovaných absolventů v univerzitních městech<br>Expanze do dalších významných univerzitních měst v ČR<br>Možnost snížení závislosti na cizích licencích vlastní produkcí | Větší pravděpodobnost „nováčkovských chyb“ u zaměstnanců<br>Nízká organizovanost destabilizuje rozvoj firmy<br>Nízká organizovanost zvyšuje riziko bezpečnostních incidentů (nejen v IT prostředí)<br>Dlouhodobější paralyzace soudního systému komplikuje bezpečnou expanzi do SR |

### 2.4.1 Silné stránky

Hlavní silnou stránkou je zaměření společnosti – cílem je prodávat především mladším lidem, zejména studentům. Z této skupiny lidí také firma vybírá své zaměstnance – prodejem výrobku a marketingovou kampaní tak zvyšuje své povědomí u potenciálních zaměstnanců. Mladší zaměstnanci jsou energičtí, ochotní vymýšlet nové postupy. To snižuje celkový odpor zaměstnanců vůči změnám.

### 2.4.2 Slabé stránky

Nábor zaměstnanců z řad absolventů má i nevýhodu – nezkušenost. Do nových zaměstnanců je potřeba ze začátku více investovat, aby začali efektivně vykonávat svoji činnost. Největším problémem ale je malá míra organizace ve společnosti – procesy nejsou formalizované, probíhají stále stejným způsobem jako při založení firmy. Stagnace je zřejmá i v IT technologiích, u kterých se zvyšuje riziko bezpečnostních incidentů.

### 2.4.3 Příležitosti

Díky tomu, že zaměstnance vybírá společnost především ze své klientely, najde firma snadněji nové zaměstnance a může relativně snadno expandovat – geograficky, personálně i produktově. Kreativita a celkově ochota zaměstnanců inovovat usnadní posílení vlastní značky, která v tuto chvíli není příliš známá.

### 2.4.4 Hrozby

Největší hrozbou je vznik bezpečnostních incidentů. Zvláště velké riziko vidím v oblasti IT, kde oddělení ztrácí povědomí o uživatelských účtech, jejich rozsahu oprávnění a

platnosti. Při současné míře neorganizovanosti hrozí firmě úpadek vlivem zvyšování výdajů na řešení bezpečnostních incidentů.

## 2.5 IT oddělení a IT prostředí

Všichni interní zaměstnanci IT oddělení se nachází v sídle společnosti v Praze. Toto oddělení poskytuje služby všem výdejnám.

### 2.5.1 Užívané systémy

Společnost používá adresářovou službu Active Directory, která funguje na systému MS Windows server 2012. Dále využívá ERP systém Money S5, který se skládá z několika vzájemně propojených modulů (účetnictví, produkce, bankovnictví, HR apod.). Veškeré transakce jsou uchovávány v interně vyvinutém systému Admin a do systému Money S5 jsou posílány pravidelnými batchovými joby. Systém Admin používá službu 389 Directory Server pro autentizaci a autorizaci. Tato služba funguje na operačním systému CentOS – volně dostupné Linuxové distribuci založené na RedHat Enterprise Linuxu. 389 Directory server využívá databází MySQL.

Dalším užívaným systémem je DWH (Data Warehouse – datový sklad), který je outsourcovaný společností Anon DW.

Společnost plánuje zavést service desk, konkrétně řešení ServiceNow.

### 2.5.2 Outsourcing

Všechny servery jsou outsourcovány formou IaaS společností Anon Hosting. Tato společnost také poskytuje firewalling-as-a-service a ochranu proti DDoS útokům.

Společnost Anon DW, poskytuje datový sklad formou SaaS. Společnost Anon Support poskytuje aplikační podporu aplikace Money S5.

Společnost plánuje využití vlastních serverů a migraci veškerých dat z externích zdrojů na interní. Výjimkou je datový sklad, který zůstane plně pod kontrolou vendora. Migrace probíhá nezávisle na této práci.

### 2.5.3 Certifikace

Společnost nemá žádnou certifikaci související s IT technologiemi ani nepoužívá žádnou metodiku (COBIT, COSO apod.). Společnost neplánuje žádné změny v této oblasti.

## 2.6 Autentizace

V této kapitole rozeberu proces autentizace pro adresářové služby, aplikační a databázovou vrstvu.

### 2.6.1 Adresářové služby

Politika hesel pro adresářové služby není nijak formalizována v interních směrnicích společnosti.

Active Directory (AD) nemá definovanou politiku hesel. AD je využíváno pouze pro autorizaci uživatelů do pracovních stanic a tiskáren.

389 Directory server autentizuje uživatele podle jména a hesla. Následující politika hesel je aplikována pro všechny uživatele:

**Tabulka 2: Politika hesel na 389 Directory server**

(Zdroj: 20)

| | |
|---|---|
| **Password length** | 8 characters |
| **Password complexity requirements** | Enabled (uppercase, lowercase, digits) |
| **Password change interval** | **N/A** |
| **Password history** | **N/A** |
| **Account lockout** | **N/A** |
| **Minimum password age** | **0 days** |

### 2.6.2 Aplikační vrstva

Politika hesel pro aplikace není nijak formalizována v interních směrnicích společnosti.

Aplikace Admin nemá nastavenou vlastní politiku hesel – uživatelé jsou autentizováni přes službu 389 Directory server (politika hesel do této služby je popsána výše).Autentizace pro Money S5 probíhá s pomocí jména a hesla. Politika hesel je pro všechny uživatele nastavena podobným způsobem jako politika pro 389 Directory server – s výjimkou podmínek pro komplexitu hesla, kde je nutné do hesla zahrnout i speciální znak:

**Tabulka 3: Politika hesel pro Money S5**

(Zdroj: 21)

| | |
|---|---|
| **Password length** | 8 characters |
| **Password complexity requirements** | Enabled (uppercase, lowercase, digits, special characters) |
| **Password change interval** | **N/A** |
| **Password history** | **N/A** |
| **Account lockout** | **N/A** |
| **Minimum password age** | **0 days** |

Politika hesel do datového skladu je nastavena a spravována poskytovatelem Anon DW. Následující politika hesel je nastavena pro všechny uživatele:

**Tabulka 4: Politika hesel pro DWH**

(Zdroj: 22)

| | |
|---|---|
| **Password length** | 7 characters |
| **Password complexity requirements** | Enabled (uppercase, lowercase, digits) |
| **Password change interval** | **N/A** |
| **Password history** | **N/A** |
| **Account lockout** | **N/A** |
| **Minimum password age** | **0 days** |

### 2.6.3 Databázová vrstva

Pro přístup do MySQL není nastavený žádný autentizační mechanismus. Aplikační vrstva má pouze technický účet s vlastním heslem, který má právo aktualizovat databázi. V databázové vrstvě je „root“ účet pro údržbu databáze a jeden účet limitovaný na SQL SELECT příkazy. Žádné další účty zde nejsou.

## 2.7 Správa uživatelských účtů

V této podkapitole analyzuji procesy zakládání, údržbu a rušení nových uživatelských účtů ve společnosti + revizi rozsahu a platnosti jejich oprávnění v adresářových službách a na aplikační a databázové vrstvě

### 2.7.1 Adresářové služby

Nastoupí-li nový zaměstnanec do společnosti, HR oddělení pošle notifikaci a zažádá telefonicky o přidělení účtu a přístupových práv. Vedoucí týmu, do kterého má nový zaměstnanec nastoupit, může zajít na IT oddělení osobně s tímto požadavkem. Ani jeden z procesů není řádně formalizován – neexistuje oficiální papírová nebo elektronická forma. IT oddělení přiřazuje uživateli oprávnění na základě pozice zaměstnance, nebo na základě ústní dohody s vedoucím týmu.

Změny v oprávnění jsou řešeny podobným způsobem – vedoucí příslušného týmu žádá o změnu oprávnění pro daného zaměstnance. Stará oprávnění se ruší a přidělují se nová.

Odchozí zaměstnanec vyplní výstupní list, obsahující všechny jeho přístupy a odevzdá jej IT oddělení. To musí na základě tohoto listu všechny přístupy odebrat a potvrdit odebrání podpisem výstupního listu.

Ve společnosti neprobíhá žádná revize uživatelských oprávnění ani dormantů. Toto platí pro Active Directory i 389 Directory server

### 2.7.2 Aplikační vrstva

Proces přidělování, změn i odebírání uživatelských oprávnění v aplikaci Admin a Money S5 se shoduje s procesy u adresářových služeb.

Ve společnosti neprobíhá žádná revize uživatelských oprávnění ani dormantů. Toto platí pro všechny aplikace s výjimkou datového skladu. Zde dělá revizi externí zaměstnanec společnosti Anon DW. Nicméně tato revize se týká optimalizace licencí, ne uživatelských oprávnění. Revize probíhá měsíčně a výstup z ní není nijak formalizován.

### 2.7.3 Databázová vrstva

Na databázové vrstvě se nezakládají žádné účty a proces přidělování a odebírání práv není aplikovatelný nad technickými účty.

## 2.8 Privilegované účty

V této podkapitole analyzuji správu privilegovaných účtů ve společnosti

### 2.8.1 Autentizace

Autentizační procesy pro privilegované účty se neliší od procesů pro běžné účty, včetně aplikované politiky hesel.

### 2.8.2 Defaultní a sdílené administrátorské účty

V žádné z aplikací ani adresářových nejsou defaultní administrátorské účty uzamčené ani přejmenované. Tyto účty jsou příležitostně využívány za účelem správy aplikace. Hesla

k nim znají pouze správci jednotlivých aplikací (každý správce zná heslo administrátorského účtu pro svoji aplikaci) a vedoucí IT oddělení. Hesla nejsou žádným způsobem uložena v žádné podobě, v případě náhlého odchodu vedoucího a správce dané aplikace hrozí ztracení přístupu k defaultním účtům natrvalo.

V systému Money S5 se nachází sdílený privilegovaný účet AdminIT, využívaný dvěma zaměstnanci IT oddělení poskytovatele.

### 2.8.3 Privilegovaný přístup vývojářů do produkčního prostředí

Společnost má 3 vývojáře, všichni mají privilegovaný přístup do produkčního prostředí a společně se správci aplikací jsou oprávnění implementovat vyvinuté změny. Implementaci příležitostně provádí správci aplikací jen příležitostně, většinu změn implementují vývojáři.

### 2.8.4 Externí účty

Vendor Anon Support poskytuje aplikační podporu aplikace Money S5. Pro zajištění podpory je v systému přidán účet AnonSupport, který má administrátorský přístup. Účet by měl být používán dvěma osobami, ale společnost nemá tuto informaci uvedenou ve smlouvě s poskytovatelem služby, ani nemá uvedeno, o koho se jedná.

Účet za normálních okolností není přístupný. Zaměstnanec vendora musí nejprve požádat správce aplikace emailem o přidělení přístupu. Přístup je přidělen na omezenou dobu, většinou na 24 hodin. Přestože účet by měl být využíván 2 osobami, žadatelé o přístup byli za poslední rok 3.

Datový sklad je plně pod správou společnosti Anon DW.

## 2.9 Požadavky společnosti

Vedení společnosti vnímá potřebu změnit vnitřní prostředí společnosti a přeje si formalizovat interní procesy týkající se identity managementu. V rámci politiky hesel si vedení přeje implementaci protokolu Kerberos, včetně navržení schématu pro jednotné přihlášení a nastavení politiky hesel pro centrální autentizační bod pro běžné i privilegované a servisní účty.

Pro správu uživatelských účtů si společnost přeje standardizovat a formalizovat procesy přidělování, změny a odebírání uživatelských oprávnění. Společnost uvítá zavedení dodatečných kontrol pro prevenci výskytu dormantů a účtů s nepotřebným rozsahem oprávnění. Do procesů by měl být zahrnut nový service desk portál ServiceNow.

Primárním cílem společnosti je formalizace procesů týkajících se správy identit pro vytvoření jasného přehledu odpovědností v rámci jednotlivých procesů. V tomto ohledu uvítá společnost návrhy i mimo již zmíněné oblasti, např. pro privilegované účty nebo procesy zahrnující externí poskytovatele služeb.

Druhotným požadavkem je zajištění transparentnosti procesů správy uživatelských účtů pro potřeby auditu, tj. pro každý proces správy uživatelských účtů musí být způsob ověření fungování těchto procesů ze zdrojů HR oddělení.

## 2.10 Zhodnocení současného stavu

Na základě analýzy hodnotím situaci ve společnosti jako velmi špatnou. Politika hesel u systému nastavuje buď velmi slabou úroveň zabezpečení hesla, nebo vůbec neexistuje. Interní směrnice pro politiku hesel neexistují pro žádný systém.

Společnost nijak neformalizovala interní procesy týkající se přidělování, změny a rušení uživatelských účtů a oprávnění. Dodržování zavedených postupů ve firmě se děje pouze na základě dobré vůle a v případě problémů není možné dodržování těchto postupů

vynutit. Vzhledem k tomu, že se počet zaměstnanců každoročně zvyšuje, roste i riziko ztráty kontroly nad zaměstnanci.

Společnost neprovádí žádné relevantní revize uživatelských oprávnění a dormantů. Hrozí tak neoprávněný přístup odchozího zaměstnance, kterému při odchodu ze společnosti nebudou z jakéhokoli důvodu odebrána přístupová práva.

Správci aplikací používají defaultní administrátorské účty. V systému Money S5 se nachází sdílený privilegovaný účet vendora, ale společnost neví, kdo přes účet může přistupovat, o tomto dostala pouze neformální ujištění. Ve smlouvě není určena odpovědnost za tento účet a za případné škody, které může uživatel tohoto účtu způsobit. Dalším problémem v rámci privilegovaných přístupů je přístup vývojářů do produkčního prostředí – vývojáři mohou implementovat jakoukoli jimi vyvinutou změnu.

Společnost nevnímá systém správy identit jako celek a má zavedené pouze některé dílčí procesy, nezbytné pro fungování systémů. Společnost vznikla jako startup projekt s velmi nízkou úrovni byrokracie. Podstatou úspěšného rozvoje každého podniku je ve správnou chvíli přejít na více organizovanou strukturu pro zajištění stability. Společnost styl řízení změnila od svého vzniku jen minimálně. Na základě SWOT analýzy považuji nápravu výše zmíněných nedostatků za krok ke zvýšení úrovně organizovanosti ve společnosti.

# 3 Návrh řešení

V této kapitole navrhnu na základě analýzy současného stavu nové řešení.

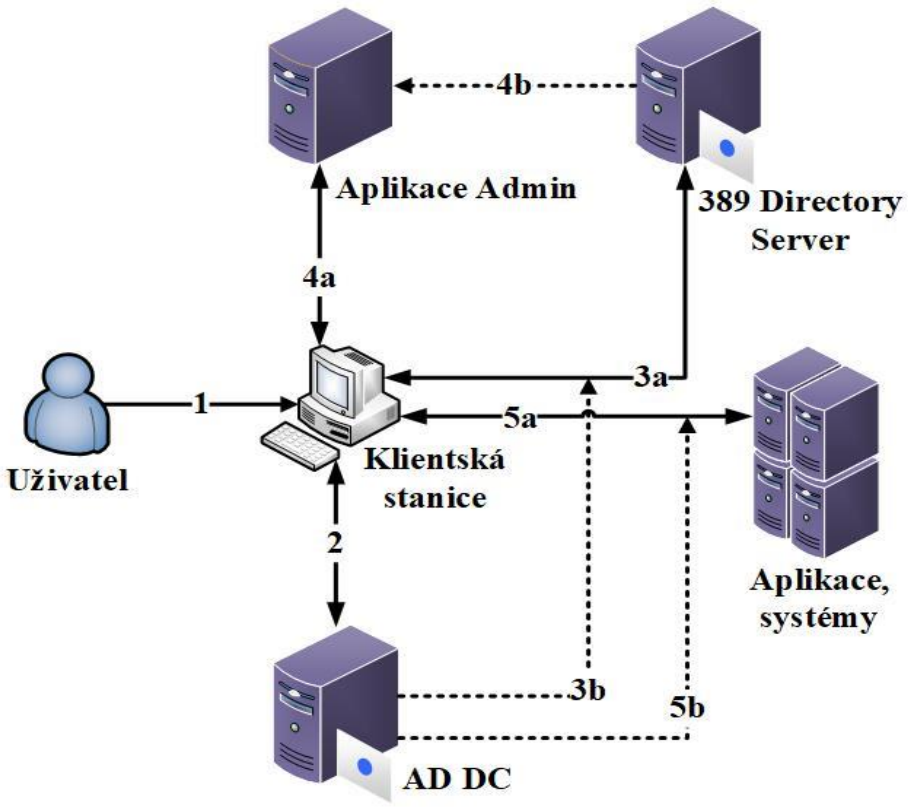
## 3.1 Návrh autentizačních procesů

V této podkapitole navrhnu nové autentizační procesy a postupy ve společnosti, včetně návrhů na jejich formalizaci.

### 3.1.1 Zavedení SSO

Zavedení SSO není z hlediska bezpečnosti dobré řešení pro firmu, která outsourcuje veškeré své servery. Po migraci bude implementace SSO menším bezpečnostním rizikem, proto doporučuji s implementací následujícího návrhu počkat do dokončení migrace.

V současnosti používá společnost 2 adresářové služby – Active Directory a 389 Directory Server. Užitím keytab souboru je možné pro 389 Directory Server nastavit autentizaci protokolem Kerberos pro zajištění jednotného přihlašování [23]. Proces bude oproti standardní implementaci SSO složitější, ale plně bude využíván pouze vývojáři aplikace Admin a několika neprivilegovanými uživateli. Schéma propojení aplikací bude následující:




**Obr. 9: Proces přihlašování uživatele do systémů**

(Zdroj: Vlastní tvorba)

Ve fázi 1 se uživatel přihlásí do PC a dojde k autentizaci vůči doméně (2). Výstupem pro klienta je Kerberos ticket, který může být použit k autentizaci vůči službě 389 Directory Server. Fyzicky komunikuje klientská stanice (3a), logicky v komunikaci figuruje i DC, který prostřednictvím klienta předá adresářové službě Kerberos ticket (3b). Po autentizaci může klient přistoupit k aplikaci Admin (4a), je autorizovaný 389 Directory Serverem (4b). Přístup k ostatním aplikacím a službám v rámci domény (5a, 5b) probíhá stejný způsobem jako kroky 3a, 3b.

Kroky 3a, 3b, 4a, 4b platí jen pro uživatele s přístupem do aplikace Admin. V rámci společnosti jde o cca 10 lidí. Pro ostatní zaměstnance tyto kroky nejsou potřebné.

Výhodou tohoto postupu je snížení nároků na uživatele – jeho jedinou činností bude prvotní přihlášení do klientské stanice a otevření aplikací, ke kterým v danou chvíli potřebuje přístup. Bez SSO by uživatel musel při každé autentizaci vůči jakékoli službě

zadávat své přihlašovací údaje. Snížení nároků na uživatele usnadní zavedení silnější politiky hesel.

### 3.1.2 Návrh heslové politiky pro Active Directory

V rámci návrhu nových autentizačních procesů ve společnosti je potřeba nastavit novou politiku hesel pro Active Directory – současná nevyhovuje doporučeným standardům a neposkytuje dostatečnou formu zabezpečení

**Tabulka 5: Nová politika hesel**
(Zdroj: Vlastní tvorba)

| | |
|---|---|
| **Enforce assword history** | 12 passwords remembered |
| **Password change interval** | 0 (never expires) |
| **Minimum password age** | 2 days |
| **Password length** | 10 characters |
| **Password must meet complexity requirements** | Enabled |
| **Store passwords using reversible encryption** | Disabled |
| **Account lockout duration** | 15 minutes |
| **Account lockout threshold** | 5 invalid attempts |
| **Reset account lockout after** | 15 minutes |

Důvody pro výše zmíněné nastavení jsou následující:

Dnešní standardy běžně doporučují sílu hesla 8 znaků, s vynucenou komplexitou (minimálně jedno malé, velké písmeno a číslice) [24]. Vzhledem k tomu, že ve společnosti bude zaveden systém jednotného přihlášení (SSO, viz níže), dojde ke snížení nároků na uživatele a bude možné zesílit toto zabezpečení. Proto doporučuji nastavit minimální délku na 10 znaků s vynucenou komplexitou.

Dobu exspirace nedoporučuji nastavovat. Uživatel si v případě povinné obměny nastaví heslo podobné. Podobnost s předcházejícím heslem může usnadnit útočníkovi jeho prolomení. Doporučuji měnit jen v případě podezření na kompromitaci.

V případě, že heslo má být změněno, je potřeba zajistit použití odlišného oproti předchozím z minulosti. Běžným opatřením je nastavení historie hesel. Uživatel si heslo ale může změnit vícekrát za den – opakovaným generováním historii přepíše a může nastavit své staré heslo. Doporučuji nastavit minimální dobu trvání na 2 dny. Pro uživatele bude zapamatování si jednoho nového hesla méně náročné než průběžné generování a zapamatování si 12 hesel po dobu 24 dní. Delší minimální dobu trvání hesla nedoporučuji, uživatel by měl mít možnost si heslo změnit při podezření na kompromitaci.

Heslovou politiku pro DWH nemá společnost možnost nastavit, správa politiky hesel je plně v rukou poskytovatele. Doporučuji vyjednat s poskytovatelem zavedení silnější politiky, ideálně se stejnými parametry jako na Active Directory.

### 3.1.3 Návrh směrnic

Na základě výstupů z podkapitoly o autentizaci navrhuji nový pracovní postup:

**ÚČEL DOKUMENTU**

Postup „Uživatelská jména a hesla do systému“ za účelem zajištění správného vytváření uživatelských jmen a hesel v systémech společnosti ABC, s.r.o. (dále též „Společnost“).

**ROZSAH PLATNOSTI**

Pravidla pro tvorbu uživatelských jmen se vztahují na všechny uživatelské účty fyzických osob vytvářené pro interní potřeby.

Pravidla pro tvorbu hesel se vztahují na všechna hesla vytvářená pro potřeby společnosti.

## JMÉNA, HESLA, PRÁCE S NIMI

Přidělování hesel je jednou ze základních činností IT oddělení pro zajištění bezpečnosti IS. Umožňuje uživatelům jejich zadávání, ale nerozhoduje o jejich podobě a v žádném případě je nezapisuje místo uživatele. Ten si musí svoje hesla volit a zapisovat sám. Uživatel je také povinen používat jen svá přístupová hesla a nesdělovat je jiným.

Pro zajištění unikátnosti uživatelského jména je požadovaná struktura následující: PříjmeníOsobníČíslo

Příjmení je psané malými písmeny bez diakritiky. Základní uživatelské jméno lze doplnit i dalšími znaky, např. pro označení administrátorského účtu.

Každý uživatel je odpovědný za jím vytvořená hesla. Na jejich základě je jim podle jejich individuálního nastavení zpřístupňován určitý rozsah aplikací.

Pro uživatelské účty/přístupy jsou **minimální** podmínky pro vytvoření hesla následující:

- minimální délka 10 znaků
- heslo neobsahuje slova (jména, názvy, zkratky apod.)
- heslo zároveň obsahuje
    - 1 nebo více malých písmen
    - 1 nebo více velkých písmen
    - 1 nebo více číslic
    - může obsahovat i znaky: !@#$%^&*(){}[]

**Doporučený** způsob tvorby hesla je následující**:**

- minimální délka 20 znaků
- heslo zároveň obsahuje

- malá písmena
- velká písmena
- číslice
- může obsahovat i znaky: !@#$%^&*(){}[]
- **heslo je nesmyslná věta**

**NEDODRŽENÍ STANOVENÝCH ZÁSAD A POVINNOSTÍ**

Porušení zásad bezpečného nakládání s hesly ohrožuje data a systémy Společnosti a bude považováno za závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci dle §52 písm.g) Zákona č. 262/2006 Sb., Zákoník práce, se všemi z toho vyplývajícími důsledky.

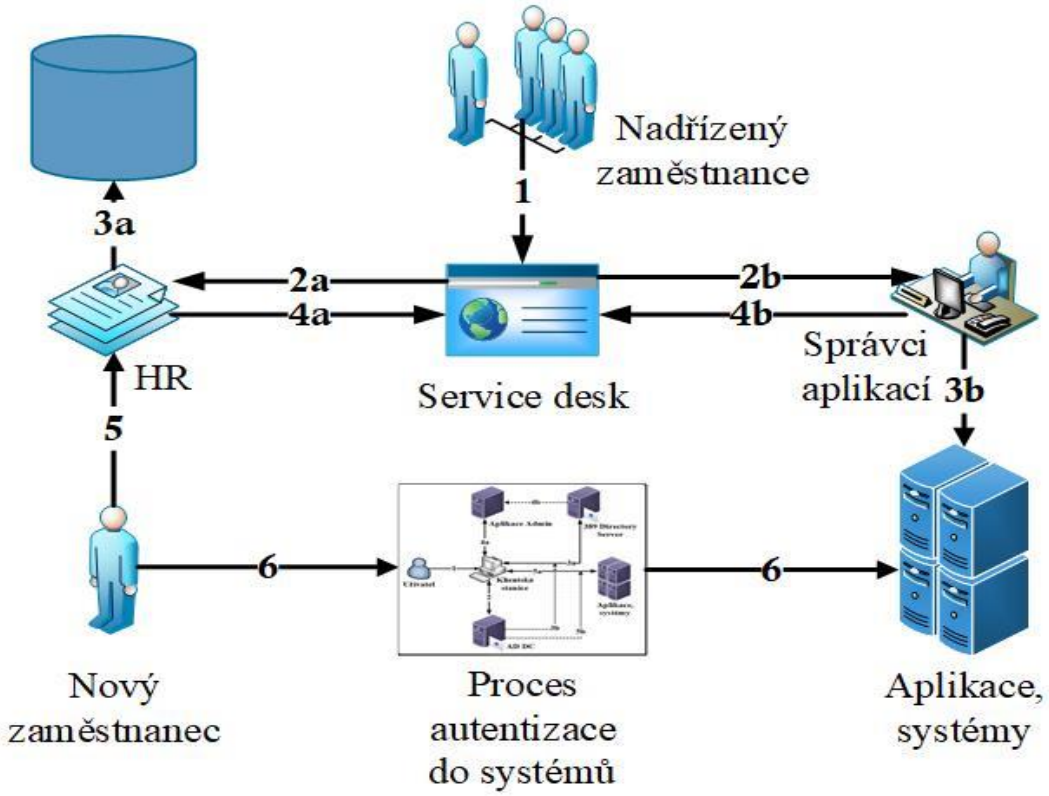
Kompletní podobu směrnice přikládám do příloh

## 3.2 Návrh procesů správy uživatelských účtů

V této podkapitole navrhnu procesy přidělování, změny a odebírání uživatelských účtů a revizi rozsahu i platnosti uživatelských oprávnění, včetně jejich formalizace.

### 3.2.1 Proces vytváření a změny uživatelských účtů

Proces přidělování uživatelských přístupů u nového nástupu je znázorněn v následujícím diagramu:




**Obr. 10: Návrh provisioning procesu**

(Zdroj: vlastní tvorba)

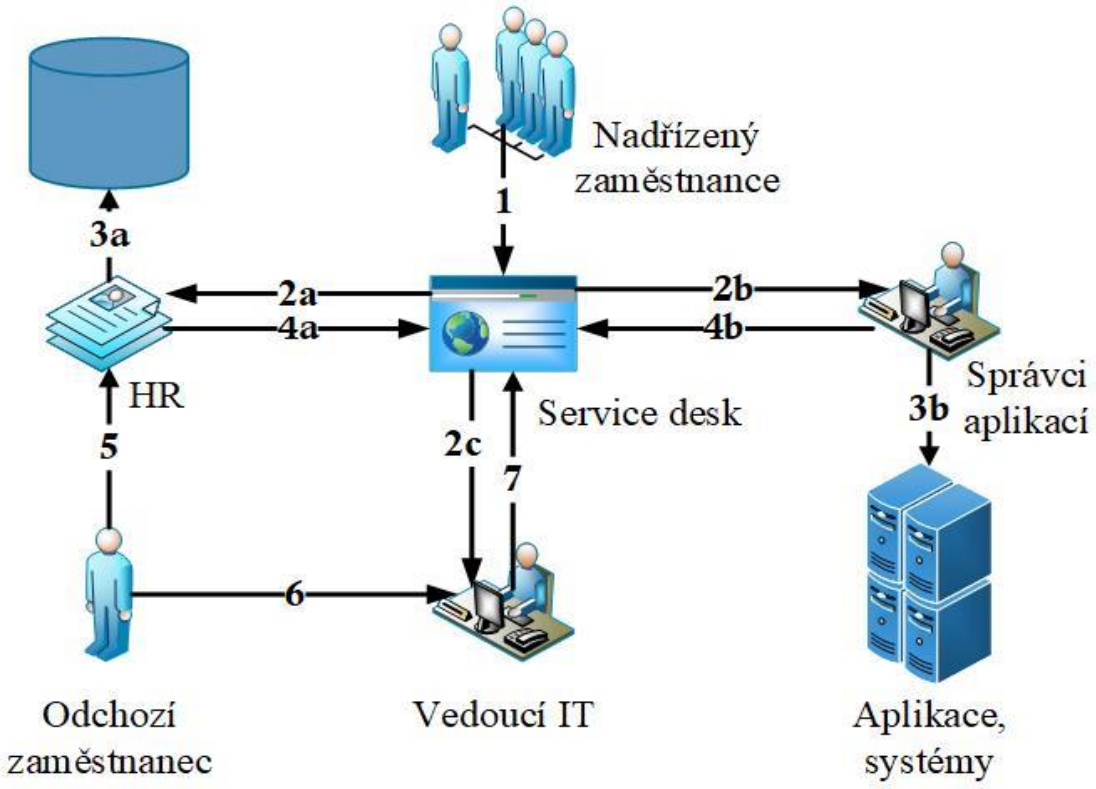
Před nástupem nového zaměstnance založí jeho formální nadřízený ticket v Service desku, specifikující pracovní pozici nového zaměstnance a uživatelská oprávnění, která bude potřebovat (1) – specifikace oprávnění bude provedena vyjmenováním všech relevantních přístupů a rolí, které uživatel potřebuje, nesmí docházet k žádostem o klonování přístupových práv podle již existujících uživatelů. Notifikace o novém ticketu bude automaticky zaslána HR oddělení (2a) a správcům aplikací (2b). HR oddělení zadá údaje do HR modulu systému Money S5 (3a), připraví smlouvy a další dokumenty pro zaměstnance k podepsání a potvrdí provedení činností v ticketu (4a). Současně správci aplikací na základě informací z ticketu nastaví zaměstnanci přístupová práva v aplikacích (3b) a potvrdí jejich vytvoření v ticketu (4b). Při nástupu zaměstnanec přijde do HR oddělní, podepíše připravené dokumenty (5) a provede proces prvního přihlášení do systému (krok 6, proces popsán v kapitole „Zavedení SSO“). Ticket je definitivně uzavřen a archivován v okamžiku úspěšného přihlášení zaměstnance do systému.

V případě změny pracovní pozice zaměstnance je proces totožný.

Přestože HR oddělení nemá přímý vliv na přidělování identit, jejich zapojení do standardizovaného procesu je klíčové pro zajištění transparentnosti.

### 3.2.2 Proces revokace uživatelských účtů

Proces revokace uživatelských přístupů u nového nástupu je znázorněn v následujícím diagramu:




**Obr. 11: Návrh de-provisioning procesu**

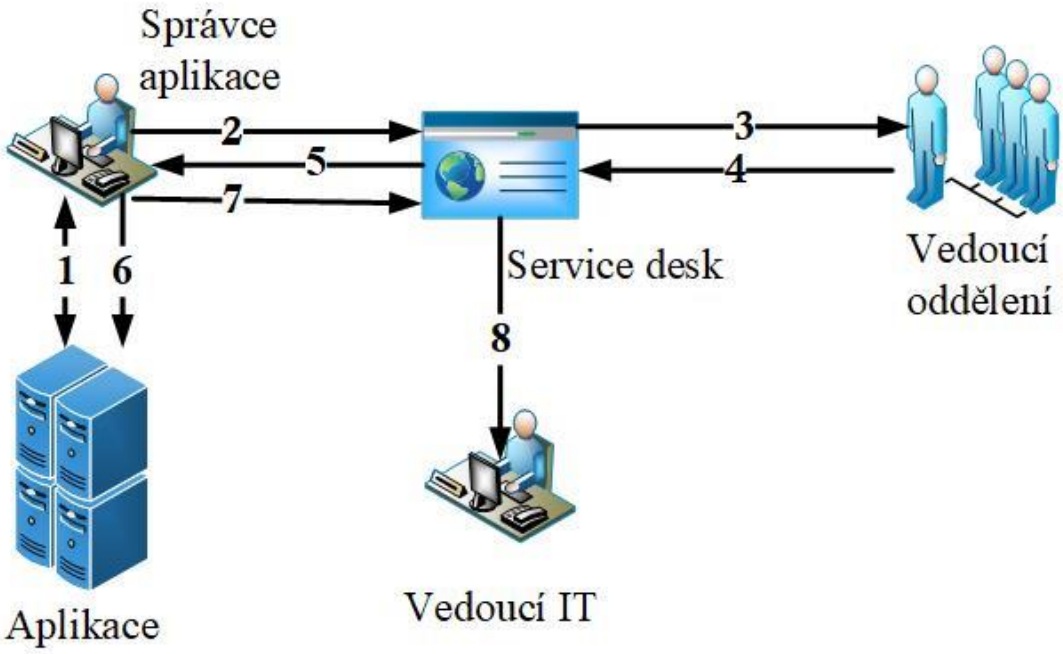
(Zdroj: vlastní tvorba)

Struktura procesu je podobná jako u vytváření účtů. Nadřízený odchozího zaměstnance, který o jeho odchodu ví zpravidla jako první, zadá ticket na Service desk (1). Ten pošle upozornění HR oddělení (2a) a oddělení IT, konkrétně správcům aplikací (2b) a vedoucímu IT oddělení (2c). HR oddělení v reakci na ticket připraví výstupní formulář a přidá zaměstnanci do HR systému datum výstupu (3a). Provedení této činnosti ohlásí

v ticketu (4a). Mezitím, správci aplikací odeberou zaměstnanci všechny jeho přístupy, pokud možno zablokováním všech účtů (ne smazáním, 3b). Zrušení přístupů ohlásí v ticketu (4b). Odchozí zaměstnanec přijde na HR oddělení a převezme výstupní formulář. S ním obejde všechna oddělení a získá potvrzení o vrácení společností poskytnutých věcí – telefon, klíče, přístupové karty, laptop atd. (není zaznačeno ve schématu – není relevantní pro proces). Součástí je i návštěva IT oddělení, kde vedoucí IT potvrdí do formuláře svým podpisem zrušení všech přístupů. IT oddělení je poslední destinací zaměstnance, proto si IT formulář ponechá, naskenuje a nahraje kopii do ticketu. V případě potřeby může formulář nahrát oddělení HR, IT manažer ale za nahrání nese odpovědnost, proto je ticket na začátku posílán jemu.

### 3.2.3 Proces revize rozsahu a platnosti uživatelských oprávnění

Proces revize uživatelských účtů a jejich oprávnění je znázorněn na následujícím diagramu:




**Obr. 12: Proces revize rozsahu a platnosti uživatelských práv**

(Zdroj: vlastní zpracování)

Revize bude probíhat jednou ročně, pro každou aplikaci zvlášť. Na začátku revize provede správce aplikace export všech uživatelských účtů a jejich oprávnění (1). Seznam pošle ve formě excelové tabulky vedoucím jednotlivých oddělení prostřednictvím ticketu v helpdesku (2, 3). Každý vedoucí se vyjádří ke všem uživatelům, kteří jsou pro jeho oddělení relevantní (4, 5). Účty lze ponechat, zrušit, nebo změnit rozsah jejich oprávnění. Na základě této revize provede správce aplikace potřebné změny (6) a provedení změn potvrdí do ticketu (7). O výsledku je informován vedoucí IT (8). Ten je účastníkem procesu už ve fázi 3 (je jedním z vedoucích oddělení). Výstup revize je relevantní pouze pro něj.

Alternativním postupem v praxi bývá pravidelné posílání seznamu odchozích zaměstnanců z HR oddělení správcům aplikací. Ti srovnáním seznamu s exportem uživatelů z aplikací provádí revizi a následně provádí potřebné změny. Tento postup nezajišťuje tzv. Segregation of duties – v tomto případě oddělení povinností mezi osobou, která reviduje a osobou, která provádí změny v systému. Zároveň v procesu není nikdo, kdo by revidoval práva správců aplikací. Proto takový proces považuji za nevhodný.

### 3.2.4 Návrh směrnic

Na základě výstupů z podkapitoly o autentizaci navrhuji novou směrnici o následujícím znění:

**ÚČEL DOKUMENTU**

Postup "Správa přístupů do informačního systému" slouží jako závazný pokyn pro přidělování, změnu a odebírání přístupových práv k informačním systémům ABC, s.r.o. (dále též „společnost“) a dále revizi jejich rozsahu a platnosti v pravidelných časových intervalech.

## ROZSAH PŮSOBNOSTI

Tento postup je závazný pro všechny zaměstnance společnosti, fyzické nebo právnické osoby, které v rámci smluvního vztahu při plnění svých úkolů u provozovatele IS přicházejí do styku s informacemi, s nimiž pracuje příslušný informační systém.

## NASTAVENÍ PŘÍSTUPOVÝCH PRÁV

Za rozsah přidělených přístupových práv odpovídá přímý nadřízený pracovníka, který je definuje se znalostí jeho pracovních povinností.

Vedoucí zaměstnanec společnosti, který stanovuje konkrétní oprávnění, je odpovědný za to, že umožní zaměstnanci "přístup“ pouze k informacím potřebným pro výkon jeho funkce. Učiní-li jinak, může to být považováno za překročení jeho pravomocí nebo porušení pracovní kázně. Veškeré spory a nejasnosti v oblasti přidělování přístupových práv řeší správce relevantní aplikace ve spolupráci s vedoucím IT oddělení.

U ostatních osob, které nejsou v pracovním poměru ve společnosti, tohoto postupu tak učiní vedoucí zaměstnanec podepisující smlouvu nebo finanční ředitel společnosti po podpisu smlouvy mezi touto osobou, osobami a společností. Vztahují se pak na ně stejné povinnosti jako na zaměstnance společnosti. Veškeré smlouvy musí obsahovat klauzuli, "že tyto osoby budou respektovat zákon 101/2000 Sb. O ochraně osobních údajů, včetně pozdějších znění a novel, a že společnost si vyhrazuje právo při porušení tohoto zákona použít sankcí uvedených v tomto zákoně".

Dále musí být ve smlouvě akceptovány požadavky na spolupráci a bezpečnostní pravidla podle ITS – 08 Pravidla spolupráce se třetími stranami v oblasti IT

Za dodržení těchto požadavků jsou odpovědni všichni zaměstnanci společnosti, kteří jsou oprávněni k podpisu smluv mezi společností, a.s. a cizím subjektem.

Přístupová práva se rozdělují na dva základní druhy.

- k datovým sítím, diskovému prostoru, jednotlivým serverům a aplikacím (představuje rozsah zpřístupněného informačního prostoru)
- k datům v rámci dané aplikace (znamená možnost pracovat s daty určitého typu a rozsahu)

Při definování přístupových práv se musí brát zřetel na různé pohledy jejich organizace.

Přístupová práva v jednotlivých aplikacích jsou koncipována podle organizační struktury, dále jsou projektově orientovaná a rozdělena podle zařazení dat do různých kategorií.

Kategorizace dat je popsána v ITS – 02 Práce s informacemi.

Pokud dojde k situaci, kdy jeden z aspektů popírá druhý, je pořadí priorit a důležitosti následující:

- kategorizace dat
- projektový přístup
- hledisko organizační struktury

Nastavení přístupových práv se provádí vytvořením ticketu v service desku. Ticket musí být adresován pracovníkům IT oddělení a také pracovníkům útvaru HR.

V rámci tohoto formuláře jsou řešeny přístupy:

- k počítačové síti společnosti
- k aplikaci a databázi systému Money S5
- k aplikaci a databázi systému Admin
- k elektronické poště a INTERNETu
- k terminálovému serveru
- vzdálený přístup (prostřednictvím bezdrátové datové sítě provozovatele mobilních služeb, nebo veřejného internetu).

Na základě ticketu provedou správci relevantních aplikací přidělení uživatelských oprávnění. Každý správce aplikace odpovídá za přidělení pravomocí odpovídajících požadavku v ticketu.

V případě podezření na příliš vysoký rozsah oprávnění v rámci požadavku je správce aplikace povinen hlásit své podezření vedoucímu IT oddělení a konzultovat s ním další kroky.

V případě, že sada oprávnění je určena novému zaměstnanci, je pracovník HR oddělení, kterému byl ticket přidělen, povinen zadat nového zaměstnance do HR modulu systému Money S5.

Každý ticket je po nastavení požadovaných služeb archivovány v rámci service desku.

## ZMĚNY V PŘÍSTUPOVÝCH PRÁVECH

Změny přístupových práv jsou prováděny prostřednictvím service desku. Ticket se žádostí pro nastavení upraveného, doplněného přístupu vyhotoví přímý nadřízený zaměstnance, který tak učiní na základě pracovního a funkčního zařazení zaměstnance. Ticket je třeba adresovat IT oddělení, jehož pracovník – správce relevantní aplikace – zajistí přidělení příslušných práv.

Změnu provede pracovník odebráním všech přístupů v dané aplikaci a nastavením přístupů nových pro zajištění prevence kumulace přístupových oprávnění.

V případě změny příjmení, zejména z důvodu změny rodinného stavu je postup následující. Není třeba opětovná žádost od přímého nadřízeného. Požadavek na změnu přístupového jména, pokud je odvozeno od příjmení, podává dotyčný pracovník. Po provedení změny je povinností správce přístupových práv doplnit do ticketu informaci „Změna příjmení z důvodu…“

## ZRUŠENÍ PŘÍSTUPU

Při ukončení pracovního poměru je povinností jeho přímého nadřízeného informovat o tom IT oddělení a útvar HR prostřednictvím ticketu v service desku. Na základě ticketu jsou správci relevantních aplikací povinni a odpovědní za zablokování všech účtů uživatele na dobu 90 dní. Po 90 dnech správci aplikací přístupy ruší, pokud tomu nebrání vlastnosti aplikace (např. kvůli zachování historie transakcí). Výjimkou je odchod zaměstnance na mateřskou dovolenou.

Dále je povinností každého zaměstnance, který využíval IS, v rámci ukončování PPV informovat o tom IT oddělení prostřednictvím předložení výstupního listu k podpisu vedoucímu IT oddělení. Ten ověří, zda došlo k ukončení platnosti přístupových práv příslušnými správci aplikací a podpisem výstupního listu potvrdí provedení tohoto úkonu.

Výstupní list je nahrán do service deskového ticketu vedoucím IT oddělení. V případě potřeby (např. dodatečného vyřizování úkonů při výstupu ze společnosti) může nahrání provést zaměstnanec HR oddělení.

U ostatních osob, které nejsou v pracovním poměru ke společnosti a jsou uvedeny v článku "Rozsah působnosti" tohoto postupu zodpovídá za zrušení přístupu k IS vedoucí zaměstnanec pověřený uzavřením smlouvy v okamžiku jejího splnění nebo ukončení její platnosti.

## REVIZE ROZSAHU A PLATNOSTI UŽIVATELSKÝCH OPRÁVNĚNÍ

V rámci pravidelných kontrolních činností vedoucích pracovníků se kontrolují i přístupová práva podřízených zaměstnanců. Proces inicializuje správce aplikace. Každý správce aplikace je povinen jednou ročně exportovat seznam všech uživatelských účtů a jejich přístupů a poslat je prostřednictvím ticketu v service desku vedoucím všech oddělení, která aplikaci využívají.

Vedoucí oddělení má povinnost vyjádřit se v rámci ticketu ke všem uživatelským účtům, které jsou, nebo byly využívány pracovníky jeho oddělení, ve smyslu, zda mají být ponechány, zneplatněny, nebo změněny. Vedoucí oddělení nese odpovědnost za toto rozhodnutí.

Na základě rozhodnutí vedoucích zaměstnanců provedou správci relevantních aplikací patřičné změny uživatelských oprávnění. V případě podezření na příliš vysoký rozsah oprávnění v rámci požadavku je správce aplikace povinen hlásit své podezření vedoucímu IT oddělení a konzultovat s ním další kroky.

**NEDODRŽENÍ STANOVENÝCH ZÁSAD A POVINNOSTÍ**

Porušení postupů správy uživatelských účtů ohrožuje data a systémy společnosti a může být považováno za závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci dle §52 písm.g) Zákona č. 262/2006 Sb., Zákoník práce, se všemi z toho vyplývajícími důsledky.

Kompletní podobu směrnice přikládám do příloh

## 3.3 Privilegované účty

V této podkapitole navrhnu opatření pro zabezpečení privilegovaných účtů ve společnosti, včetně návrhu úprav relevantních směrnic.

### 3.3.1 Autentizační procesy

Privilegované účty vyžadují vyšší úroveň zabezpečení a osoby, které je využívají, jsou v rámci svého pracovního zaměření alespoň částečně seznámeni s problematikou

informační a kybernetické bezpečnosti. Proto považuji za vhodné nastavit politiku hesel pro privilegované účty s následujícím rozdílem oproti politice pro běžné uživatele:

**Tabulka 6: Úprava politiky hesel pro privilegované účty**
(Zdroj: Vlastní tvorba)

| | |
|---|---|
| **Password length** | **16 characters** |

### 3.3.2 Defaultní a sdílené administrátorské účty

Defaultní účty jsou častým cílem útoků. Doporučuji přestat používat a deaktivovat defaultní účty tam, kde je to možné – především v Active Directory. Zároveň doporučuji zrušit všechny sdílené účty, které brání zajištění nepopiratelnosti v případě napáchání škody. Doporučuji zavést pouze jmenné administrátorské účty, které budou přiřazeny konkrétní osobě a budou využívány výhradně pro administrátorské účely (více viz segregace administrátorských a běžných účtů).

Pro zajištění dostupnosti administrátorských účtů v případě nouze, doporučuji uložit hesla k nejsilnějším privilegovaným účtům v papírové podobě. Výtisky uloží správci aplikací do obálek a předají vedoucímu IT oddělení. Ten uloží výtisky do trezoru. Toto opatření doporučuji pro případ náhlé ztráty znalosti hesla k nejsilnějším účtům (např. nedostupnost administrátora ze zdravotních důvodů).

### 3.3.3 Segregace administrátorských a běžných účtů

Správci aplikací budou mít jeden administrátorský účet a jeden běžný účet pro běžné úkony pro zajištění minimalizace privilegií uživatele – administrátorské účty budou používány výhradně pro potřebné úkony. Správci aplikací už běžné účty mají, po zavedení administrátorského jim běžné musí být ponechány.

### 3.3.4 Přístup vývojářů do produkčního prostředí

Vývojáři implementují jimi navržené změny. Jde o velké bezpečnostní riziko, vývojáři mohou implementovat do systému škodlivý kód bez vědomí jiné osoby ve společnosti. Doporučuji zrušit privilegovaný přístup vývojářů do produkčního prostředí a přidělit odpovědnost za implementaci změn správcům aplikací. Dále doporučuji upravit směrnice pro změnové řízení ve společnosti, aby byla zmíněná pravidla formalizována a byla vynucena odpovědnost za jejich nedodržování. Návrh směrnic změnového řízení spadá do jiné oblasti informační bezpečnosti a není cílem této práce. Vzhledem ke vzájemné provázanosti oblastí jsem ale usoudil, že zmínění této problematiky je pro potřeby splnění cílů práce nezbytné.

### 3.3.5 Externí účty

Sdílený externí privilegovaný účet AnonSupport v aplikaci Money S5 považuji za problém. Není dosaženo nepopiratelnosti v případě spáchání škody v systému prostřednictvím tohoto účtu. Doporučuji sdílený účet zrušit a založit pro každého externího zaměstnance jeden privilegovaný jmenný účet a vynutit jejich používání úpravou smlouvy s vendorem. O přístup do systému pak mohou žádat pouze vlastníci těchto účtů.

### 3.3.6 Doplnění směrnice pro tvorbu hesel

Na základě předchozích návrhů doporučuji do směrnice o heslové politice dodat následující:

**ADMINISTRÁTORSKÁ HESLA**

Tvorba administrátorského hesla odpovídá běžnému postupu, s výjimkou minimální délky – 10 znaků je nahrazeno délkou 16 znaků.

**SYSTÉMOVÁ HESLA**

(systémová hesla/servisní účty – hesla jsou používána programy, které je čtou ze svých konfiguračních souborů, aby se připojily k doméně, databázím apod.)

Tvorba systémového hesla odpovídá běžnému postupu, s výjimkou minimální délky – 10 znaků je nahrazeno délkou 16 znaků.

Je doporučeno měnit toto heslo alespoň jednou ročně.

Kompletní podobu směrnice přikládám do příloh

### 3.3.7 Doplnění směrnice o správě uživatelských účtů

Na základě předchozích návrhů doporučuji do směrnice správě uživatelských účtů dodat následující:

**SPRÁVA PRIVILEGOVANÝCH ÚČTŮ**

Každý administrátorský účet musí být propojen s konkrétním správcem aplikace a pojmenovaný podle směrnice IdMS – 01 Uživatelská jména hesla do systému, s přidáním prefixu „adm“ k username. Účty s administrátorskými právy jsou oprávněni užívat pouze správci aplikací. Každý správce aplikace je oprávněn užívat pouze administrátorský účet k aplikaci, za kterou je odpovědný. Odpovědnost se vztahuje i na činnosti vykonané daným privilegovaným účtem. Správci aplikací jsou povinni dodržovat pravidlo

minimalizace privilegií – administrátorské účty mohou používat pouze pro činnosti vyžadující vyšší set oprávnění. Pro běžné úkony je správce povinen používat běžný účet.

Vedoucí IT oddělení je odpovědný za uchování informací o přístupech k defaultním administrátorským účtům a nejsilnějším aktivním administrátorským účtům pro případ ztráty ostatních forem znalostí hesel pro tyto účty. Každý správce aplikace je povinen předat vedoucímu IT oddělení tyto informace v papírové podobě, vložené do obálky. Vedoucí IT tuto obálku uloží do trezoru a uchová pro případ potřeby.

Kompletní podobu směrnice přikládám do příloh

## 3.4 Návrh projektu implementace systému správy identit

V této podkapitole navrhnu projekt implementace výše zmíněných návrhů změn.

### 3.4.1 Síly inicializující proces změny

Vedení firmy několik posledních let využívá služeb externího audiu účetní závěrky. Jeho součástí je i tzv. IT audit. V rámci této dodatečně poskytované služby je ve firmě analyzován stav zabezpečení informačních systémů, které jsou pro audit účetní závěrky relevantní. Výstup těchto kontrol je určen pro finanční auditory, ale i pro klienta – zde společnost ABC.

Na základě těchto výstupů vyhodnotil vedoucí IT oddělení společnosti stav zabezpečení IT prostředí ve společnosti celkově jako nevyhovující a přesvědčil generálního ředitele o nutnosti podniknout příslušná opatření. Součástí je i návrh systému správy identit pro systémy ovlivňující finanční transakce ve společnosti, s možností rozšíření implementace na všechny informační systémy ve společnosti.

### 3.4.2 Síly působící pro a proti změně

Největší vliv na vznik změny má její interní iniciátor – vedoucí IT oddělení. Výkonný ředitel společnosti si přeje zajištění interní stability podniku a změnu podporuje.

Hlavní opoziční silou je finanční oddělení a finanční ředitel společnosti. Odpor vůči změně je založen převážně na přesvědčení, že investice do IT nepřinesou v budoucnu žádný užitek. Společnost zatím neutrpěla výraznější ztrátu vlivem bezpečnostních incidentů v oblasti IT, proto nelze přesvědčit finančního ředitele o závažnosti situace. Osobní vztah s výkonným ředitelem ale snižuje riziko výraznější aktivní opozice ve financování projektu.

Pasivně odporují změně i někteří zaměstnanci IT oddělení, kvůli potenciálnímu zvýšení pracovní vytíženosti.

Shrnutí jednotlivých postojů ke změně podle matice aktivní/pasivní – podporuje/nepodporuje přikládám níže:

- Agenti změny – část IT oddělení (manažer, správci aplikací)
- Nezúčastnění diváci – oddělení nákupu, logistiky, marketingu, obsahu, HR, operační oddělení
- Tradicionalisté – část IT oddělení (IT podpora)
- Odpůrci – finanční oddělení, CFO

### 3.4.3 Agent změny

Viz předchozí podkapitola – agentem změny budou zaměstnanci IT oddělení zodpovědní za jednotlivé systémy a dále jejich vedoucí v roli koordinátora a konzultanta.

### 3.4.4 Intervenční oblasti

Implementace IdM zahrnuje větší množství dílčích úkolů. Změna procesu přidělování uživatelských přístupů ovlivní HR a IT oddělení a nově příchozí zaměstnance. Změna heslové politiky ovlivní všechny zaměstnance ve společnosti. Zavádění SSO může způsobit dočasnou nedostupnost relevantních systémů. Případné změny v řízení aplikačních změn ovlivní poskytovatele služeb k relevantním informačním systémům. Ve všech případech bude ovlivněno IT oddělení. V následujících odstavcích rozeberu intervence v oblastech podle [19]:

- Řízení lidských zdrojů
- Organizační struktura
- Technologie
- Informační a organizační toky firmy

Řízení lidských zdrojů bude ovlivněno novým procesem správy uživatelských účtů – HR oddělení bude při založení ticketu ukládat relevantní informace do svého systému. V reakci na tickety bude připravovat dokumenty pro podpis zaměstnancům. Dále bude vedoucí HR oddělení v rámci revize rozsahu uživatelských oprávnění při obdržení seznamu aktivních uživatelských účtů povinen specifikovat, zda daná oprávnění pro účty jeho podřízených zaměstnanců odpovídají jejich pracovní náplni (platí i pro všechny ostatní vedoucí ve společnosti). Všem zaměstnancům včetně HR oddělení budou resetována hesla – každý zaměstnanec bude povinen si nastavit nové podle nových interních směrnic.

K výraznějším intervencím v organizační struktuře nedojde. Zaměstnancům IT oddělení budou přiděleny dodatečné odpovědnosti – správci aplikaci budou odpovědní za provedení roční revize platnosti i rozsahu přístupových práv a implementaci dodavatelem prováděných změn do produkčního prostředí informačních systémů. Zaměstnanec IT komunikující s poskytovateli IT služeb bude informován o změnách v kontraktech s poskytovateli a bude povinen dohlížet na dodržování kontraktů ze strany dodavatelů.

Revize přístupových práv vynutí redukci rozsahu oprávnění jednotlivých uživatelů v informačních systémech pouze na rozsah stanovený organizační strukturou.

Společnost začne využívat technologii Single Sign-On (SSO) pro jednotné přihlašování do informačních systémů. U externích dodavatelů bude změnou v řízení přístupů vynucena přímá odpovědnost za jakýkoli krok, který by vedl k poškození firmy. Kvalita produktů nebude ovlivněna žádným přímým způsobem, ale dojde k redukci bezpečnostního rizika – vznik bezpečnostních incidentů by ohrozil produkci a poskytované služby z hlediska kvality i kvantity.

Informační a organizační toky ve firmě budou ovlivněny výše zmíněnými procesy správy uživatelských účtů – standardizované formuláře u nových nástupů, roční revize platnosti i rozsahu přístupových práv. Výše zmíněné povede především ke standardizaci informačních toků a tím pádem k lepší informovanosti IT oddělení o uživatelích systémů a o poskytovatelích IT služeb. Zapojení oddělení lidských zdrojů do těchto procesů zajistí ověřitelnost fungování procesů.

### 3.4.5 Proces změny

V této podkapitole rozeberu jednotlivé fáze procesu změny ve společnosti založené na Lewinově modelu změny – fázi rozmrazení, vlastní změnu a zamrazení [19].

V **první fázi** (rozmrazení) může společnost schválit design celého procesu – navrhnout definitivní podobu nových pokynů a směrnic a připravit obsah školení, která bude potřeba provést. Dále mohou být vyjednány a připraveny návrhy nových smluv s poskytovateli IT služeb. Změnami v heslové politice budou ovlivněni všichni zaměstnanci, je proto vhodné ohlásit plánované změny rozesláním emailových upozornění a oběžníků ještě před přechodem do implementační fáze.

V rámci fáze rozmrazení by měly být také zrevidovány všechny uživatelské přístupy. Důvodem je snaha o co nejdřívější zabezpečení přístupů do firemních systémů a

otestování fungování celého procesu. Tento proces zahájí zaměstnanci IT oddělení pověření provedením revize (správci aplikací). Ti exportují seznamy uživatelů a jejich oprávnění a pošlou je klíčovým uživatelům (vedoucím oddělení), kteří se vyjádří k rozsahu i platnosti všech oprávnění relevantních pro jejich oddělení. Tyto výstupy revize použijí správci aplikací v další fázi.

V **druhé fázi** dojde k implementaci řešení navržených v předchozích fázích. Na počátku budou do testovacího prostředí zavedeny všechny plánované technické změny – změna konfigurace domény, nastavení SSO a přizpůsobení relevantních aplikací. V rámci této fáze nastaví správci aplikací uživatelům oprávnění na základě výstupů z revize, provedené v předchozí fázi. Dále zaměstnanci IT oddělení provedou testování nově zavedených procesů a vyladí případné nedostatky.

Současně je potřeba začít zaškolovat zaměstnance. Nová heslová politika je aplikována na celou společnost, bude nutné proškolit všechny zaměstnance o pravidlech pro tvorbu hesel a nejjednodušších vhodných postupech, kvůli prevenci obcházení pravidel např. zapisováním hesel do papírové podoby. Školení o nových směrnicích o procesech správy uživatelských účtů se týkají IT a HR oddělení. Zaměstnanec IT odpovědný za komunikaci s poskytovateli IT služeb musí být také poučen o nových podmínkách spolupráce.

Po zaškolení zaměstnanců a nahrání nového řešení do testovacího prostředí může dojít k otestování řešení klíčovými uživateli. Testování se týká zavedení SSO. Klíčovými uživateli by měli být vedoucí jednotlivých oddělení, kteří otestují přístupy do systémů a jejich instancí, které jsou pro daná oddělení relevantní. Po vyladění chyb a nedostatků a otestování klíčovými uživateli mohou být navrhovaná řešení implementována do produkčního prostředí. Následně musí vstoupit v platnost nové směrnice, aplikované na politiku hesel. Další směrnice mohou být aktualizovány nezávisle na ostatních procesech, je vhodné je ale aplikovat co nejdříve. Dále nově dohodnuté smlouvy s poskytovateli služeb nahradí staré a budou změněny konfigurace účtů dodavatelů. Tyto konfigurační změny bude možné provést až po konfiguraci domény a jednotlivých aplikací.

Ve **třetí fázi** (zamrazení) dojde k zakotvení řešení ve společnosti a zajištění jeho účelnosti – všem uživatelům bude vynucena změna hesel a v případě potřeby budou vypracovány

nové dokumenty o přidělení uživatelských oprávnění, pokud dojde na základě revize k výraznější změně. Současně vstoupí v platnost nové smlouvy s dodavateli. Na závěr agenti změny odevzdají dokumentaci k nově dokončenému projektu výkonnému řediteli a všechny papírové výstupy projektu budou archivovány.

### 3.4.6 Verifikace dosažených výsledků

K ověření, že byly splněny všechny cíle, poslouží výsledky následujícího externího IT auditu ve společnosti. Výsledkem by mělo být uzavření všech nálezů z oblasti autentizace, správy uživatelských účtů, změnového řízení a privilegovaných přístupů z předchozích let.

### 3.4.7 Harmonogram a PERT

Pro potřeby této práce jsem vypracoval časový harmonogram projektu a síťovou analýzu metodou PERT. V následující tabulce lze najít seznam činností a jejich návazností:

**Tabulka 7: Seznam činností a návazností**

(Zdroj: vlastní tvorba)

| ID činnosti | Název činnosti | Navazuje na | Předchází činnosti |
|---|---|---|---|
| 1 | Finální návrh směrnice pro politiku hesel | | 8, 10 |
| 2 | Finální návrh směrnice pro UAM | | 11 |
| 3 | Revize přístupů – export a odeslání zaměstnancům | | 4 |
| 4 | Revize přístupů – vyhodnocení zaměstnanci | 3 | 8 |
| 5 | Vyjednání nových smluv s dodavateli | | 6, 7 |
| 6 | Příprava nových kontraktů | 5 | 12 |
| 7 | Úprava směrnice pro řízení změn | 5 | 12 |
| 8 | Návrh v testovacím prostředí | 1, 4 | 9 |
| 9 | Ladění v testovacím prostředí | 8 | 13 |
| 10 | Školení zaměstnanců – hesla | 1 | 13 |
| 11 | Školení zaměstnanců – UAM | 2 | 16 |
| 12 | Poučení zodpovědného zaměstnance IT o změnách v kontraktu a ve směrnicích | 6, 7 | 17, 18 |
| 13 | Testování klíčovými uživateli | 9, 10 | 14 |
| 14 | Implementace do produkčního prostředí | 13 | 15 |
| 15 | Schválení směrnic a uvedení v platnost – hesla | 14 | 19, 20 |
| 16 | Schválení směrnic a uvedení v platnost – UAM | 11 | 20 |
| 17 | Schválení směrnic a uvedení v platnost – řízení změn | 12 | 21 |
| 18 | Schválení smluv s dodavateli a uvedení v platnost | 12 | 21 |
| 19 | Vynucení změny hesel | 15 | 21 |
| 20 | Vypracování nových dokumentů pro přidělení uživatelských práv a podepsání uživateli | 15, 16 | 21 |
| 21 | Zamrazení – vypracování zprávy o provedení změny, předání zprávy CEO a archivace | 17, 18, 19, 20, | |

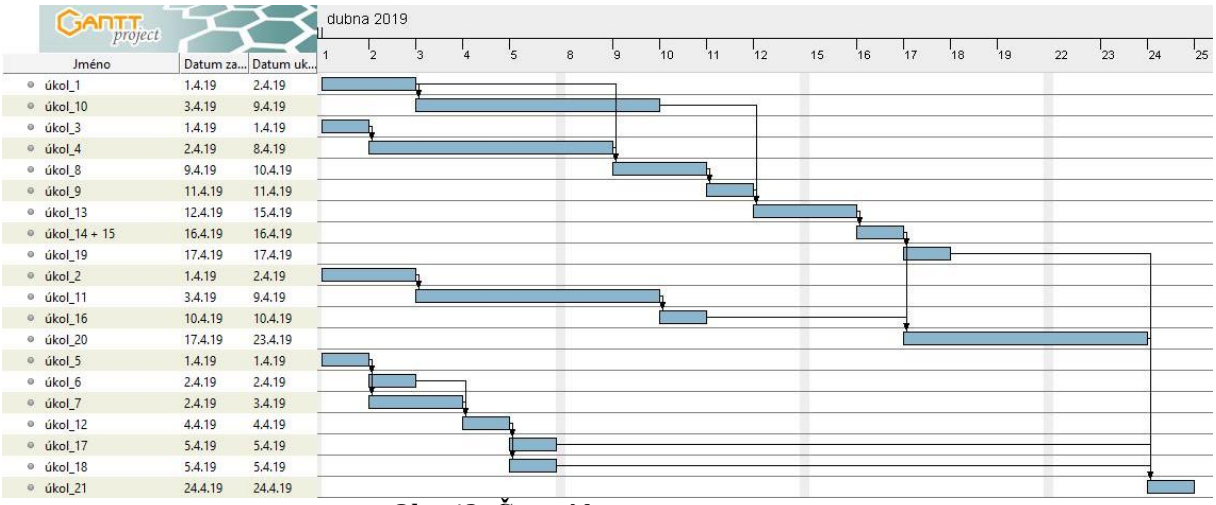
Následující tabulka obsahuje dobu trvání výše zmíněných činností:

**Tabulka 8: Doba trvání činností**

(Zdroj: Vlastní tvorba)

| ID činnosti | Optimistická doba (dny) | Realistická doba (dny) | Pesimistická doba (dny) | Střední hodnota | Rozptyl | Směrodatná odchylka |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 2,000 | 0,111 | 0,333 |
| 2 | 1 | 2 | 3 | 2,000 | 0,111 | 0,333 |
| 3 | 0,25 | 0,5 | 1 | 0,542 | 0,016 | 0,125 |
| 4 | 2 | 5 | 8 | 5,000 | 1,000 | 1,000 |
| 5 | 1 | 1 | 2 | 1,167 | 0,028 | 0,167 |
| 6 | 0,5 | 1 | 1,5 | 1,000 | 0,028 | 0,167 |
| 7 | 1 | 2 | 3 | 2,000 | 0,111 | 0,333 |
| 8 | 1 | 2 | 3 | 2,000 | 0,111 | 0,333 |
| 9 | 0,5 | 1 | 1,5 | 1,000 | 0,028 | 0,167 |
| 10 | 3 | 5 | 10 | 5,500 | 1,361 | 1,167 |
| 11 | 3 | 5 | 10 | 5,500 | 1,361 | 1,167 |
| 12 | 0,5 | 1 | 2 | 1,083 | 0,063 | 0,250 |
| 13 | 1 | 2 | 3 | 2,000 | 0,111 | 0,333 |
| 14 | 0,25 | 0,5 | 1 | 0,542 | 0,016 | 0,125 |
| 15 | 0,5 | 0,5 | 0,5 | 0,500 | 0,000 | 0,000 |
| 16 | 0,5 | 0,5 | 0,5 | 0,500 | 0,000 | 0,000 |
| 17 | 0,5 | 0,5 | 0,5 | 0,500 | 0,000 | 0,000 |
| 18 | 1 | 1 | 2 | 1,167 | 0,028 | 0,167 |
| 19 | 0,5 | 0,5 | 0,5 | 0,500 | 0,000 | 0,000 |
| 20 | 3 | 5 | 8 | 5,167 | 0,694 | 0,833 |
| 21 | 0,5 | 1 | 2 | 1,083 | 0,063 | 0,250 |

Na základě předchozích tabulek jsem sestavil časový harmonogram a provedl síťovou analýzu metodou PERT:



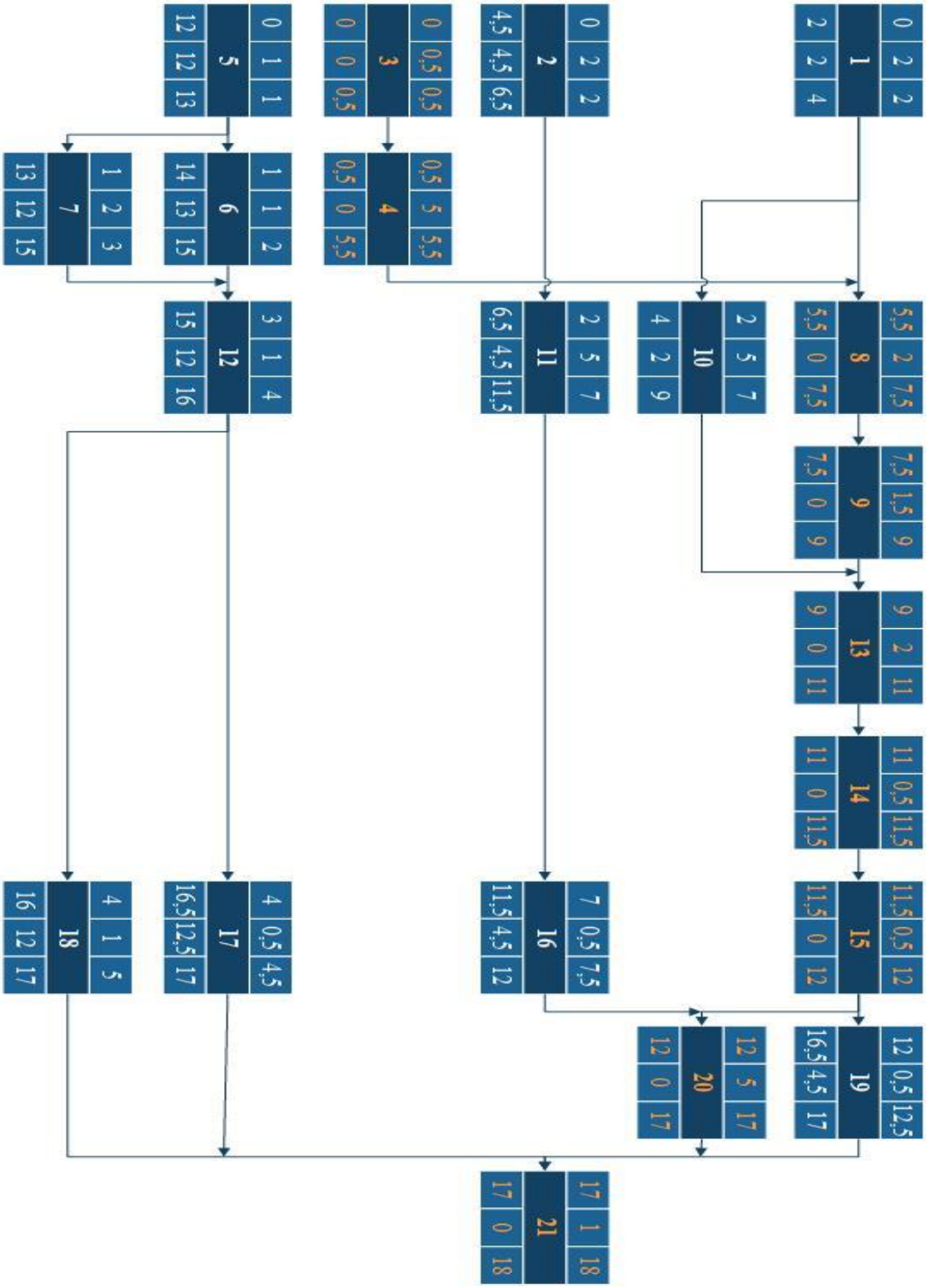

**Obr. 13: Časový harmonogram**

(Zdroj: Vlastní tvorba)

V harmonogramu jsou zahrnuty i procesy úpravy směrnic týkajících se řízení změn. Bylo zmíněno, že optimalizace řízení změn nepatří mezi cíle práce. Po dohodě s agentem změny bylo dohodnuto, že změna privilegovaných přístupů v oblasti vývojářských přístupů do produkčního prostředí bude zahrnuta do projektu jako dílčí činnost.

Z modelu PERT (viz níže) je výstupem odhad délky projektu – 18 pracovních dní. Po vložení projektu do programu Gantt project a sestavení harmonogramu se zahrnutím víkendů vychází, že při zahájení projektu 1. dubna by očekávané dokončení projektu bylo 24. dubna.

Kritická cesta vede přes činnosti: 3-4-8-9-13-14-15-20-21




**Obr. 14: Síťová analýza metodou PERT**

(Zdroj: Vlastní tvorba)

## 3.5 Řízení rizik

V této kapitole provedu analýzu rizik, které v průběhu implementace změny mohou ohrozit integritu nebo včasné dokončení projektu změny. V první části identifikuji rizika a scénáře. V dalších podkapitolách posoudím jejich pravděpodobnost a závažnost a na závěr navrhnu opatření pro tato rizika a sestavím mapu rizik před a po zavedení opatření.

### 3.5.1 Identifikace hrozeb a scénářů

Na základě analýz vnitřních i vnějších faktorů jsem identifikoval následující rizika:

**Tabulka 9: Analýza rizik**

(Zdroj: Vlastní tvorba)

| ID rizika | Hrozba | Scénář |
|---|---|---|
| **1** | Špatně vypracovaná analýza projektu změny | Zpoždění nebo zdražení projektu oproti plánu |
| **2** | Nesprávná konfigurace domény při finální implementaci | Prodloužení odstavení domény – nefunkčnost aplikací |
| **3** | Odchod agentů změny z firmy | Zpoždění projektu |
| **4** | Špatné nastavení privilegovaných přístupů do aplikací | Bezpečnostní incident |
| **5** | Nedostatečné zaškolení zaměstnanců | Ztráta účelnosti projektu – uživatelé budou nové procesy ignorovat |
| **6** | Dodavatel nebude souhlasit s novými podmínkami | Ztráta kontraktu |
| **7** | Některý z vedoucích oddělení nepředá informace potřebné pro zrevidování přístupů | Zpoždění projektu, bezpečnostní incident |

### 3.5.2 Hodnocení rizik

Pro potřeby tohoto projektu jsem vytvořil tabulky pro určení pravděpodobnosti, dopadu a následného vyhodnocení závažnosti. Na jejich základě ohodnotím jednotlivá rizika.

**Tabulka 10: Hodnocení rizik**

(Zdroj: Vlastní tvorba)

| Pravděpodobnost | | Dopad | | Označení hodnoty |
|---|---|---|---|---|
| **Zanedbatelná** | 0-20 % | **Zanedbatelný** | 0-5 000 Kč | 1 |
| **Nízká** | 21-40 % | **Nízký** | 5 001-10 000 Kč | 2 |
| **Střední** | 41-60 % | **Střední** | 10 001-20 000 Kč | 3 |
| **Vysoká** | 61-80 % | **Vysoký** | 20 001-50 000 Kč | 4 |
| **Kritická** | 81-100 % | **Kritický** | 50 001 a více Kč | 5 |

**Tabulka 11: Tabulka pro určení hodnoty rizika**

(Zdroj: Vlastní tvorba)

| Pravděpodobnost/dopad | Zanedbatelný | Nízký | Střední | Vysoký | Kritický |
|---|---|---|---|---|---|
| **Zanedbatelná** | 1 | 2 | 3 | 4 | 5 |
| **Nízká** | 2 | 4 | 6 | 8 | 10 |
| **Střední** | 3 | 6 | 9 | 12 | 15 |
| **Vysoká** | 4 | 8 | 12 | 16 | 20 |
| **Kritická** | 5 | 10 | 15 | 20 | 25 |

**Tabulka 12: Popis hodnocení rizik**

(Zdroj: Vlastní tvorba)

| Závažnost rizika | Hodnota rizika |
|---|---|
| Zanedbatelná | 1-3 |
| Nízká | 4-6 |
| Střední | 7-10 |
| Vysoká | 11-19 |
| Kritická | 20-25 |

Na základě těchto teoretických tabulek jsem ohodnotil jednotlivá rizika:

**Tabulka 13: Hodnocení rizik**

(Zdroj: Vlastní tvorba)

| ID rizika | Pravděpodobnost | Dopad | Hodnota rizika |
|---|---|---|---|
| 1 | 2 | 3 | **6** |
| 2 | 1 | 3 | **3** |
| 3 | 1 | 4 | **4** |
| 4 | 2 | 5 | **10** |
| 5 | 3 | 4 | **12** |
| 6 | 2 | 5 | **10** |
| 7 | 4 | 5 | **20** |

### 3.5.3 Snižování rizik

V této podkapitole navrhnu opatření pro řízení rizik z předchozích podkapitol.

**Tabulka 14: Možnosti snížení rizik s novými hodnotami rizika**

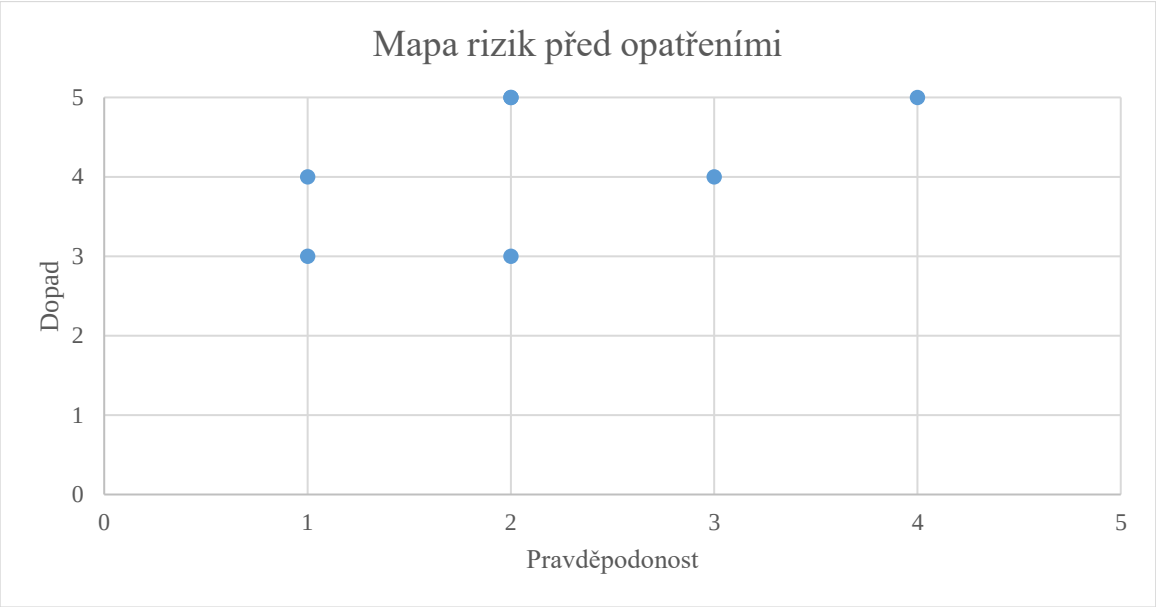
(Zdroj: Vlastní tvorba)

| ID | Způsob řízení rizika | Původní hodnota rizika | Nová pst. | Nový dopad | Nová hodnota rizika | Náklady na opatření | Odpovědná osoba |
|---|---|---|---|---|---|---|---|
| **1** | Revize vedoucím IT oddělení | 6 | 1 | 3 | 3 | 3 000 – 5 000 Kč | Vedoucí IT oddělení |
| **2** | Akceptace rizika | 3 | 1 | 3 | 3 | 0 Kč | - |
| **3** | Akceptace rizika | 4 | 1 | 4 | 4 | 0 Kč | - |
| **4** | Revize vedoucím IT oddělení | 10 | 1 | 2 | 2 | 3 000 – 5 000 Kč | Vedoucí IT oddělení |
| **5** | Zavedení povinného absolvování testů | 12 | 2 | 3 | 6 | 2 000 – 3 000 Kč | Správce domény |
| **6** | Připravení podkladů pro jednání se záložním dodavatelem | 10 | 2 | 2 | 4 | 2 500 – 4 000 Kč | Jednatel za stranu žadatele |
| **7** | Včasné upozornění vedoucích a jejich uvědomění o potenciální způsobené škodě | 20 | 3 | 3 | 9 | 0 – 1 000 Kč | Správci aplikací |

Opatření pro rizika většinou nejsou nákladná. Jejich hodnota se odvíjí od průměrných mezd v oboru, ve kterém odpovědná osoba působí a odhadované doby trvání přípravy opatření. Žádné opatření nevyžaduje více než jeden pracovní den práce.

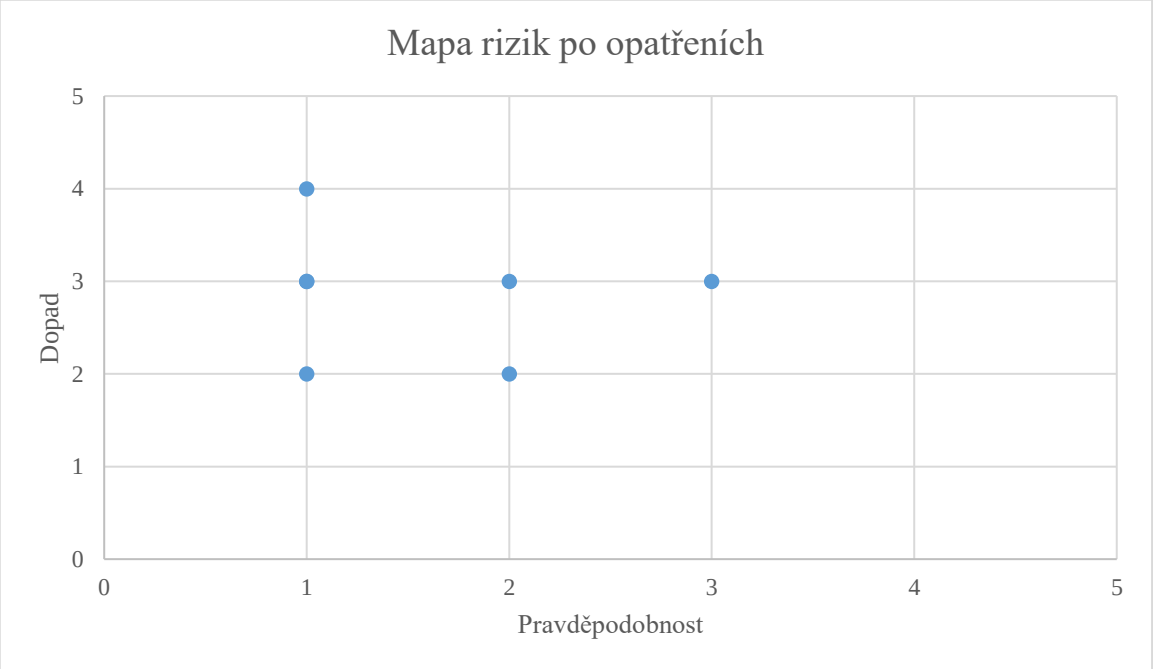
### 3.5.4 Mapa rizik

Na základě předchozích údajů jsem vypracoval mapu rizik před a po zavedení opatření:




**Graf 1: Mapa rizik před zavedením opatření**

(Zdroj: Vlastní tvorba)




**Graf 2: Mapa rizik po zavedení opatření**

(Zdroj: Vlastní tvorba)

### 3.5.5 Zhodnocení analýzy rizik

Analýza odhalila 7 rizik. 2 rizika jsou nevýznamná, nevyplatí se investovat do opatření. Pro zbylých 5 byla navržena vhodná opatření. Cena opatření pro rizika se odvíjí od průměrných mezd v oboru, ve kterém odpovědná osoba působí a odhadované doby trvání přípravy opatření. Žádné opatření nevyžaduje více než jeden pracovní den práce.

Výsledkem zavedení opatření je snížení pravděpodobnosti u všech rizik na maximálně 40 %. U některých rizik se podařilo také zredukovat dopad (ztráta dodavatele má nyní dopad podstatně nižší, díky přípravě nouzového plánu na jednání se záložním dodavatelem) Konečným důsledkem je zmírnění všech závažných rizik na maximálně střední závažnost

## 3.6 Ekonomické zhodnocení

Náklady projektu tvoří především mzdy odpovědných zaměstnanců, ostatní zdroje má firma k dispozici (servery, software apod.), nebo jsou zanedbatelné (tisk dokumentů), případně jejich nasazení je součástí jiných projektů (Service desk). Finanční zhodnocení jednotlivých činností v rámci projektu uvádím v následující tabulce:

**Tabulka 15: Náklady projektu**

(Zdroj: Vlastní zpracování)

| ID činnosti | Realistická doba trvání* (člověkodny) | Odpovědná osoba | Přibližná měsíční mzda odpovědné osoby (Kč) | Náklady (Kč) |
|---|---|---|---|---|
| 1 | 2 | Vedoucí IT | 100 000 | 9 524 |
| 2 | 2 | Vedoucí IT | 100 000 | 9 524 |
| 3 | 2 | 4x Správci aplikací | 60 000 | 5 714 |
| 4 | 4 | 8x Vedoucí oddělení | 85 000 | 16 190 |
| 5 | 1 | Vedoucí IT | 100 000 | 4 762 |
| 6 | 1 | Vedoucí IT | 100 000 | 4 762 |
| 7 | 2 | Vedoucí IT | 100 000 | 9 524 |
| 8 | 2 | Správce domény | 60 000 | 5 714 |
| 9 | 1 | Správce domény | 60 000 | 2 857 |
| 10 | 4 | Správce domény | 60 000 | 11 429 |
| 11 | 1,5 | Vedoucí IT | 100 000 | 7 143 |
| 12 | 0,25 | Vedoucí IT | 100 000 | 1 190 |
| 13 | 2 | 8x Vedoucí oddělení | 85 000 | 8 095 |
| 14 | 2 | 4x Správci aplikací | 60 000 | 5 714 |
| 19 | 0,125 | Správce domény | 60 000 | 357 |
| 20 | 12 | 4x Správci aplikací | 60 000 | 34 285 |
| 21 | 1 | Vedoucí IT | 100 000 | 4 762 |

*Ekonomické zhodnocení bere v potaz pouze reálně vynaloženou činnost. Vzhledem k časovým dispozicím, ne každý provede danou činnost okamžitě. To způsobuje prodloužení doby trvání některých činností v návrhu projektu oproti ekonomickému zhodnocení.

Kroky 15-18 jsou okamžité, pouze v rámci projektu je pro ně vyhrazen časový interval z důvodu potenciální časové indispozice odpovědné osoby. V ekonomickém zhodnocení proto nejsou tyto kroky zahrnuty.

Celkové odhadované náklady projektu činí 141 546 Kč. Bez existence formalizovaného procesu správy identit hrozí společnosti vysoké finanční ztráty vlivem potenciálních bezpečnostních incidentů. Z tohoto důvodu shledávám projekt z ekonomického hlediska vhodným pro realizaci.

# ZÁVĚR

Cílem této práce bylo vylepšit systém správy identit ve společnosti ABC, s.r.o. z hlediska formalizace, standardizace i kvality technických řešení takovým způsobem, aby došlo ke zvýšení bezpečnosti a snížení uživatelské náročnosti každodenních procesů, zajištění informovanosti všech zaujatých stran v rámci společnosti a zajištění transparentnosti pro externí subjekty, např. auditory. Dalším cílem bylo zajistit bezproblémovou implementaci prostřednictvím metod projektového řízení, včetně řízení potenciálních rizik.

Všechny cíle práce byly splněny. Nastavením nové, silnější politiky hesel, bylo dosaženo zvýšení bezpečnosti v systémech a navržením pravidel pro správu privilegovaných účtů bylo dosaženo vyšší úrovně zabezpečení kritických aktiv, stejně jako zajištění nepopiratelnosti. Zavedením SSO došlo ke snížení uživatelské náročnosti každodenního procesu přihlašování do systémů. Navržením procesů správy uživatelských účtů, návrhem směrnic a přidělením odpovědností byla vylepšena úroveň standardizace a zajištěna informovanost IT i HR oddělení. Zapojení oddělení lidských zdrojů do standardizovaných procesů správy identit zajistí věrohodný zdroj informací pro ověření dodržování stanovených postupů v IT oddělení pro potřeby interního i externího auditu. Byl proveden návrh implementace formou časového harmonogramu a síťovou analýzou, včetně popisu vlivu projektu implementace na prostředí firmy. Analýzou a řízením rizik byla zmírněna všechna rizika, která výrazněji ohrožovala dodržení termínů nebo rozpočtu projektu.

# SEZNAM POUŽITÝCH ZDROJŮ


[1] NGN Identity Management Framework: Recommendation Y.2720. Paris: International Telecommunication Union, 2009.

[2] BISHOP, Matt. Computer security: art and science. Boston: Addison-Wesley, c2003. ISBN 02-014-4099-7.

[3] BERTINO, Elisa a Kenji TAKAHASHI. Identity management: concepts, technologies, and systems. Boston: Artech House, 2011. Artech House information security and privacy series. ISBN 16-080-7039-5.

[4] LÍZNER, Martin. Identity management: centrální správa uživatelských účtů. Computerworld [online]. Praha, 2010 [cit. 2018-12-12]. Dostupné z: http://computerworld.cz/securityworld/identity-management-centralni-spravauzivatelskych-uctu-47568

[5] STAMP, Mark. Information security principles and practice [online]. Hoboken, N.J: Wiley-Interscience, 2005, s. 153-176 [cit. cit. 2018-12-12]. ISBN 9780471744191. Dostupné z: http://onlinelibrary.wiley.com.ezproxy.lib.vutbr.cz/doi/10.1002/0471744190.ch7/pdf

[6] ORLOWSKA, M. E. Service-oriented computing--ICSOC 2003: First International Conference, Trento, Italy, December 15-18, 2003 : proceedings [online]. New York: Springer, 2003 [cit. 2019-04-23]. ISBN 978-3-540-20681-1.

[7] NORIS, Ivan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (4. díl): Provisioning. IT SYSTEMS [online]. 2015, (5) [cit. 2016-11-27]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-provisioning.htm

[8] BALÁŽIK, Milan. Principy řízení identit. IT SYSTEMS [online]. 2015, (1-2) [cit.

2018-12-13]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/it-security/principy-rizeni-identit.htm

[9] COOPER, D. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF, 2008. Dostupné také z: https://tools.ietf.org/html/rfc5280

[10] FARRELL, S. a R. HOUSLEY. RFC 3281: An Internet Attribute Certificate Profile for Authorization. IETF, 2002. Dostupné také z: https://www.ietf.org/rfc/rfc3281.txt

[11] CHILDERS, Lisa, Rebeca CORTAZAR, Ian FORSTER, Leon KUNTZ a Jesus MARCO. GSI: Grid Security Infrastructure: Delegation and single sign-on (proxy certificates) [online]. [cit. 2019-04-22]. Dostupné z: https://docs.huihoo.com/globus/gt3-tutorial/ch11s02.html

[12] Proceedings of the 2005 workshop on Digital identity management – DIM '05 [online]. New York, New York, USA: ACM Press, 2005 [cit. 2019-04-22]. ISBN 1595932321. Dostupné z: http://portal.acm.org/citation.cfm?doid=1102486.1102500

[13] BOUŠKA, Petr. Princip Kerberos autentizace. www.samuraj-cz.com [online]. 2014 [cit. 2018-12-15]. Dostupné z: https://www.samuraj-cz.com/clanek/kerberos-cast-5-princip-kerberos-autentizace/

[14] TSAUR, Woei-Jiunn a Jia-Xin WU. A Secure Agent-based Single Sign-On Scheme Supporting Web Services Home Network Environments [online]. Taiwan, 2014 [cit. 2019-04-27]. Dostupné z: https://pdfs.semanticscholar.org/9a13/272759bac716e51654812460fc1fce8c25b1.pdf. Technická zpráva. Da-Yeh University, Department of Information Management.

[15] LIANG, Zhigang a Yuhai CHEN. The Design and Implementation of Single Sign-on Based on Hybrid Architecture [online]. Guangzhou, China, 2012 [cit. 2019-04-24]. Dostupné z:

https://pdfs.semanticscholar.org/d220/edf7ecd3355110d20a8fd6b84b56a0ff7f13.pdf . Technická zpráva. South China University of Technology.

[16] CHADWICK, David W. a George INMAN. Attribute Aggregation in Federated Identity Management. Computer [online]. 2009, 42(5), 33-40 [cit. 2019-04-19]. DOI: 10.1109/MC.2009.143. ISSN 0018-9162. Dostupné z: http://ieeexplore.ieee.org/document/5070036/

[17] SAML Specifications. SAML XML.org [online]. OASIS, 2005 [cit. 2019-04-21]. Dostupné z: http://saml.xml.org/saml-specifications

[18] Benefits of OpenID. OpenID [online]. Seattle: OpenID Foundation, 2005 [cit. 2019-04-29]. Dostupné z: https://openid.net/individuals/

[19] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada). ISBN 978-80-247-3051-6.

[20] Nastavení politiky hesel na 389 Directory Server. Praha, 2018.

[21] Nastavení politiky hesel na Money S5. Praha, 2018.

[22] Nastavení politiky hesel na DWH. Praha, 2018.

[23] BOUŠKA, Petr. Kerberos část 9 - Keytab (key table) soubor. www.samuraj-cz.com [online]. 2014 [cit. 2019-04-16]. Dostupné z: https://www.samuraj-cz.com/clanek/kerberos-cast-9-keytab-key-table-soubor/

[24] NIST SPECIAL PUBLICATION 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. USA: U.S. Department of Commerce, 2017. Dostupné také z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[25] Organizační struktura společnosti. Praha, 2018.

# SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

AD Active Directory – adresářová služba od společnosti Microsoft

AS Authentication Server – autentizační server, prvek protokolu Kerberos

DC Domain Controller – doménový řadič

DWH Data Warehouse – datový sklad

HR Human Resource – lidské zdroje

IaaS Infrastructure as a Service – forma poskytování služeb, infrastruktura formou služby

ICT Information and Communication Technologies – informačně-komunikační technologie

IdM Identity Management – správa identit

IdMS Identity Management Směrnice – sada interních směrnic společnosti ABC zabývající se správou identit ve společnosti

ISMS Information Security Management Systém – systém řízení bezpečnosti informací

ISO International Organization for Standardization – Mezinárodní organizace pro standardizaci

ITS – sada interních směrnic společnosti ABC, zabývající se postupy a procesy v IT, resp. ICT prostředí

ITU International Telecommunication Union – Mezinárodní telekomunikační unie

KDC Key Distribution Centre – součást protokolu Kerberos

PIN Personal Identification Number – osobní identifikační číslo

RBAC Role-Based Access Control – řízení přístupů na základě rolí

SaaS Software as a Service – způsob poskytování služeb, software formou služby

SAML Security Assertion Markup Language – řešení v oblasti identity managementu

SESAME Secure European System for Applications in a Multi-vendor Environment – technologie pro jednotné přihlašování

SLEPT analýza – analýza vnějšího prostředí podniku

SQL Structured Query Language – strukturovaný dotazovací jazyk, určený pro práci s daty v relačních databázích

SSO Single Sign-On – metoda jednotného přihlášení

SWOT analýza – analýza silných a slabých stránek podniku, identifikace příležitostí a hrozeb

TGS Ticket-Granting Server – server, poskytující tickety, součást protokolu Kerberos

TGT Ticket Granting Ticket – ticket udělovaný v rámci autentizace v protokolu Kerberos

URI Uniform Resource Identifier – textový řetězec, jednotný identifikátor zdroje

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# SEZNAM GRAFŮ

# SEZNAM PŘÍLOH